Warranty Registration: register online today for a chance to win a FREE Tripp Lite product—www.tripplite.com/warranty

Owner's Manual

IP Remote Access Unit

Model:
B051-000

Tested To Comply With FCC Standards

FCC Information

This is an FCC Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

This equipment has been tested and found to comply within the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at their own expense.

RoHS

This product is RoHS compliant.

Package Contents

The B051-000 package consists of:

- (1) B051-000 IP Remote Access Unit
- (1) USB KVM Cable Kit
- (1) PS/2 KVM Cable Kit
- (1) USB – PS/2 Console Connector Kit
- (1) USB 2.0 Virtual Media Cable
- (1) Power Adapter
- (1) Rackmounting Kit
- (1) Software CD with Owner's Manual
- (1) Quick Start Guide

Tripp Lite World Headquarters
1111 W. 35th Street, Chicago, IL 60609 USA
www.tripplite.com/support

Note: Follow these instructions to ensure proper operation and prevent damage to this device and its connected equipment.

Table of Contents

Table of Contents

Introduction

Features

- Provides IP Access to KVM switches or servers that do not have built-in IP functionality.
- Virtual media via USB 2.0 data transmission.
- Precision mouse-pointer syncing ability for USB mice.
- Up to 64 user accounts.
- Up to 32 concurrent user logins for single-bus sharing.
- Message board feature allows users to communicate with each other, and allows a user to take exclusive control of the KVM switch.
- Supports RADIUS, LDAPS and MS Active Directory.
- Export/import user account and configuration settings directly to the B051-000 IP Remote Access Unit.
- Access a KVM switch or server via your web browser using Windows or Java based applications.
- Supports non-browser access via Windows GUI or Java Client software.
- Supports TCP/IP, HTTP, HTTPS, UDP, DHCP, SSL, ARP, DNS, ICMP, CHAP, PPP, 10Base-T and 100Base-T.
- Superior video resolution: up to 1600 x 1200 @ 60Hz; 24-bit color depth for remote sessions.
- Optimize bandwidth using grayscale and other video quality settings.
- PPP mode (modem) dialup support for out-of-band, and low bandwidth operation.
- Allows for full-screen or sizable remote desktop window.
- In full-screen mode the remote desktop display scales to user's monitor display size.
- Advanced security features include password protection and advanced encryption technologies.
- Secure 128-bit SSL encryption.
- Enable/disable browser operation.
- Event logging.
- Remote firmware upgrading.

System Requirements

- It is recommended that the computers used to access the B051-000 IP Remote Access Unit have at least a Pentium III, 1GHz processor, and that the screen resolution is set to 1024 x 768.
- Browsers must support 128-bit data encryption.
- It is recommended that the user have an internet connection speed of at least 128 kbps.
- In order to access the Windows Client link, your browser must support ActiveX.
- You must be running Sun's Java Runtime Environment (JRE) 6, Update 3 or higher in order to access the browser-based Java Applet and AP Java Client.
- Microsoft Jet OLEDB 4.0 or higher driver must be installed to access the Log Server.

Video

Only the following non-interlaced video signals are supported:

Resolution	Refresh Rates
640 x 480	60, 72, 75, 85, 90, 100, 120
720 x 400	70
800 x 600	56, 60, 72, 75, 85, 90, 100, 120
1024 x 768	60, 70, 75, 85, 90, 100
1152 x 864	60, 70, 75, 85
1280 x 1024	60, 70, 75, 85
1600 x 1200	60

Introduction

Cables

- A KVM cable kit is required to connect the B051-000 to a KVM switch or server. (1) PS/2 KVM cable kit and (1) USB KVM cable kit is included with the unit.

Note: If the included KVM cable kit is too short, Tripp Lite has P774-Series (PS/2) and P776-Series (USB) KVM Kits available in extended lengths.

- A console connector kit is required to connect a local console to the B051-000 IP Remote Access Unit. A USB – PS/2 Console connector kit is included with the unit.
- A USB 2.0 A to Mini-B 5-Pin device cable (included) is required for use with the Virtual Media function.
- Tripp Lite Cat5e (N001- or N002-Series) or Cat6 (N201-Series) cable (not included), should be used to connect the B051-000 IP Remote Access Unit to a network.

Operating Systems

- Supported operating systems for computers/servers that are connected to the B051-000, or are connected to a KVM switch that is connected to the B051-000, are shown:
- Computer/servers remotely accessing the B051-000 must have Windows 2000 or higher, or an operating system that is capable of running Sun's Java Runtime Environment (JRE) 6, Update 3 or higher.

Operating System	Version
Windows	2000 and higher
Linux RedHat	7.1 and higher
Linux Fedora	Core 5 and higher
Linux SuSE	9.0 and higher
Linux Mandriva (Mandrake)	9.0 and higher
UNIX AIX	4.3 and higher
UNIX FreeBSD	3.51 and higher
UNIX Sun	Solaris 8 and higher
Novell Netware	5.0 and higher
Mac	OS 9 and higher
DOS	6.2 and higher

Note: The operating systems in the table above are supported by the B051-000 only. Any KVM switch connected to the B051-000 must be compatible with them as well, or the system will not function properly.

Browsers

Supported browsers for users that are accessing the B051-000 remotely include the following:

Browser	Version
Internet Explorer	6 and higher
Firefox	1.5 and higher
Mozilla	1.7 and higher
Safari	2.0 and higher
Opera	9.0 and higher
Netscape	8.1 and higher

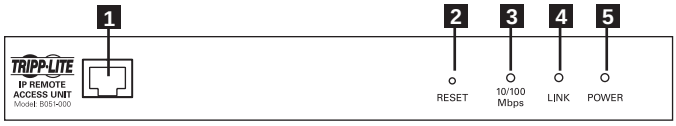
Virtual Media Support

- USB CD-ROM/DVD-ROM Drives.
- USB Floppy Drives.
- USB Flash Drives.
- IDE CD-ROM/DVD-ROM Drives.
- Image Files (.iso).

Introduction

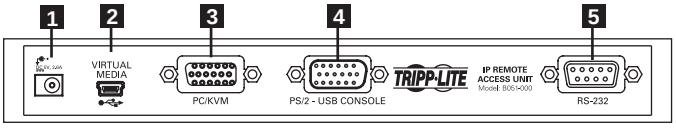
Components

Front View



No.	Component	Description
1	LAN Port	The Cat5e/6 cable that connects the B051-000 to a network plugs in here.
2	Reset Switch	1. Pressing and releasing this switch will perform a system reset. 2. Pressing and holding the switch for more than 3 seconds restores the B051-000 to its factory default configuration settings. 3. Pressing and holding this switch while powering the unit on will restore the factory default firmware version. This operation should only be performed in the event of a firmware upgrade failure that results in the device becoming inoperable. *Note: This switch is recessed and must be pushed with a thin object, such as the end of a paper clip or ballpoint pen*.
3	10/100 Mbps LED	This LED lights Orange to indicate a data transmission speed of 10Mbps, or Green to indicate a Data transmission speed of 100 Mbps.
4	Link LED	This LED flashes Green to indicate that the B051-000 is being accessed remotely.
5	Power LED	This LED lights Orange when the B051-000 is powered-on and ready to operate.

Rear View



No.	Component	Description
1	Power Jack	The included power adapter connects to the unit here.
2	Virtual Media Port	The included USB 2.0 device cable connects here when using the Virtual Media feature.
3	PC/KVM Port	The KVM cable kit that connects the B051-000 to a KVM switch or server connects to the unit here.
4	Console port	The console connector kit that connects a Local Console to the B051-000 connects to the unit here.
5	RS-232 port	An RS-232 serial port is provided for out-of-band and low bandwidth modem and serial terminal connections.

Hardware Setup

Safety Instructions

- Read all of these instructions before proceeding. Save them for future reference.

General Safety Instructions

- Follow all warnings and instructions marked on the device.
- Do not place the device on any unstable surface. If the device falls, serious damage may result.
- Do not use the device near water.
- Do not place the device near, or over, radiators or heat registers.
- Never spill liquid of any kind on the device.
- The device cabinet is provided with slots and openings to allow for adequate ventilation. To ensure reliable operation, and to protect against overheating, these openings must never be blocked or covered.
- The device should never be placed on a soft surface (bed, sofa, rug, etc.) as this will block its ventilation openings. Likewise, the device should not be placed in a built in enclosure unless adequate ventilation has been provided.
- Unplug the device from the wall outlet before cleaning. Do not use liquid or aerosol cleaners. Use a damp cloth for cleaning.
- The device should be operated from the type of power source indicated on the marking label. If you are not sure of the type of power available, consult your dealer or local power company.
- To prevent damage to your installation it is important that all devices are properly grounded.
- Do not allow anything to rest on the power cord or cables. Route the power cord and cables so that they cannot be stepped on or tripped over.
- If an extension cord is used with this device make sure that the total of the ampere ratings of all products used on this cord does not exceed the extension cord ampere rating. Make sure that the total of all products plugged into the wall outlet does not exceed 15 amperes.
- It is recommended that you plug your device into a Tripp Lite Surge Suppressor, UPS or Line Conditioner to help protect your system from sudden, transient increases and decreases in electrical power.
- When connecting or disconnecting power to hot-pluggable power supplies, observe the following guidelines:
  - Install the power supply before connecting the power cable to the power supply.
  - Unplug the power cable before removing the power supply.
  - If the system has multiple sources of power, disconnect power from the system by unplugging all power cables from the power supplies.
- Never push objects of any kind into or through any openings on the unit. They may touch dangerous voltage points or short out parts resulting in a risk of fire or electrical shock.
- Do not attempt to service the device yourself. Refer all servicing to qualified service personnel.
- If the following conditions occur, unplug the device from the wall outlet and bring it to qualified service personnel for repair:
  - The power cord or plug has become damaged or frayed.
  - Liquid has been spilled into the device.
  - The device has been exposed to rain or water.
  - The device has been dropped, or the cabinet has been damaged.
  - The device exhibits a distinct change in performance, indicating a need for service.
  - The device does not operate normally when the operating instructions are followed.
- Only adjust those controls that are covered in the operating instructions. Improper adjustment of other controls may result in damage that will require extensive work by a qualified technician to repair.
- Use of this equipment in life support applications where failure of this equipment can reasonably be expected to cause the failure of the life support equipment or to significantly affect its safety or effectiveness is not recommended. Do not use this equipment in the presence of a flammable anesthetic mixture with air, oxygen or nitrous oxide.

Rack Mounting Safety Instructions

- Before working on the rack, make sure that the stabilizers are secured to the rack, extended to the floor, and that the full weight of the rack rests on the floor. Install front and side stabilizers on a single rack or front stabilizers for joined multiple racks before working on the rack.
- Always load the rack from the bottom up, and load the heaviest item in the rack first.
- Always load the rack so that a hazardous condition is not created due to uneven loading.
- Make sure that the rack is level and stable before extending a device from the rack.

Hardware Setup

Safety Instructions *(continued)*

- Do not overload the AC supply branch circuit that provides power to the rack. The total rack load should not exceed 80 percent of the branch circuit rating.
- Make sure that all equipment used on the rack – including power strips and other electrical connectors – is properly grounded.
- Ensure that proper airflow is provided to devices in the rack.
- Ensure that the operating ambient temperature of the rack environment does not exceed the maximum ambient temperature specified for the equipment by the manufacturer (0° to 50° C).
- Do not step on or stand on any device when servicing other devices in a rack.

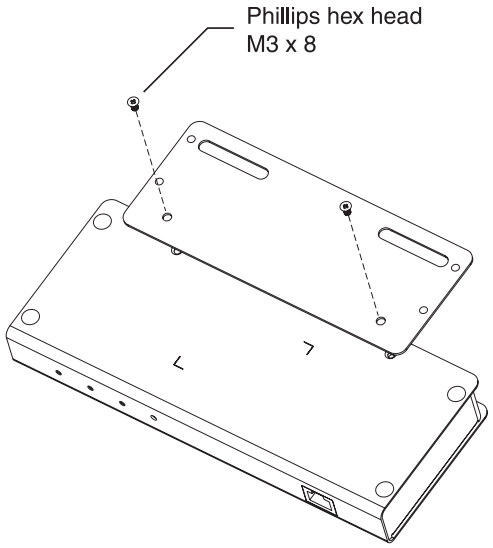
Setup Instructions

Rack Mounting

For convenience and flexibility, the B051-000 comes with a 0U rackmount kit so the unit can be conveniently mounted on a system rack.

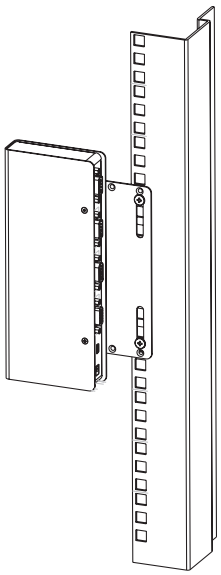
To rack mount the unit do the following:

1. Remove the two original screws from the bottom of the unit (near the rear of the unit).
2. Using the screws and bracket provided with the rack mount kit, screw the mounting bracket into the B051-000 – as shown in the diagram below.



3. Screw the bracket into any convenient location on the rack.

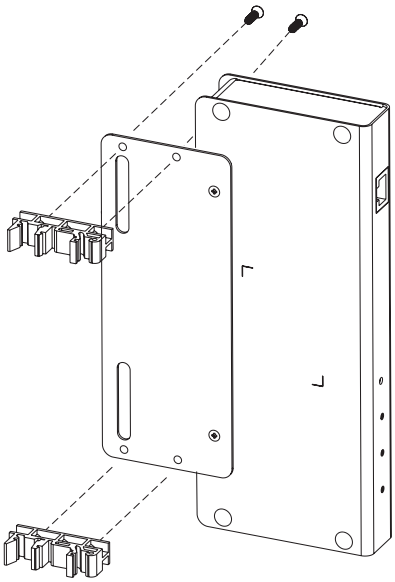
Note: Rack screws are not provided. Use screws that are appropriate for your rack.



DIN Rail Mounting

To mount the B051-000 on a DIN rail:

1. Screw the mounting bracket to the back of the B051-000 as described in steps 1 and 2 of the Rack Mounting Section.
2. Use the larger screws supplied with the Rack Mount Kit to screw the DIN rail brackets to the mounting bracket – as shown in the diagram below:



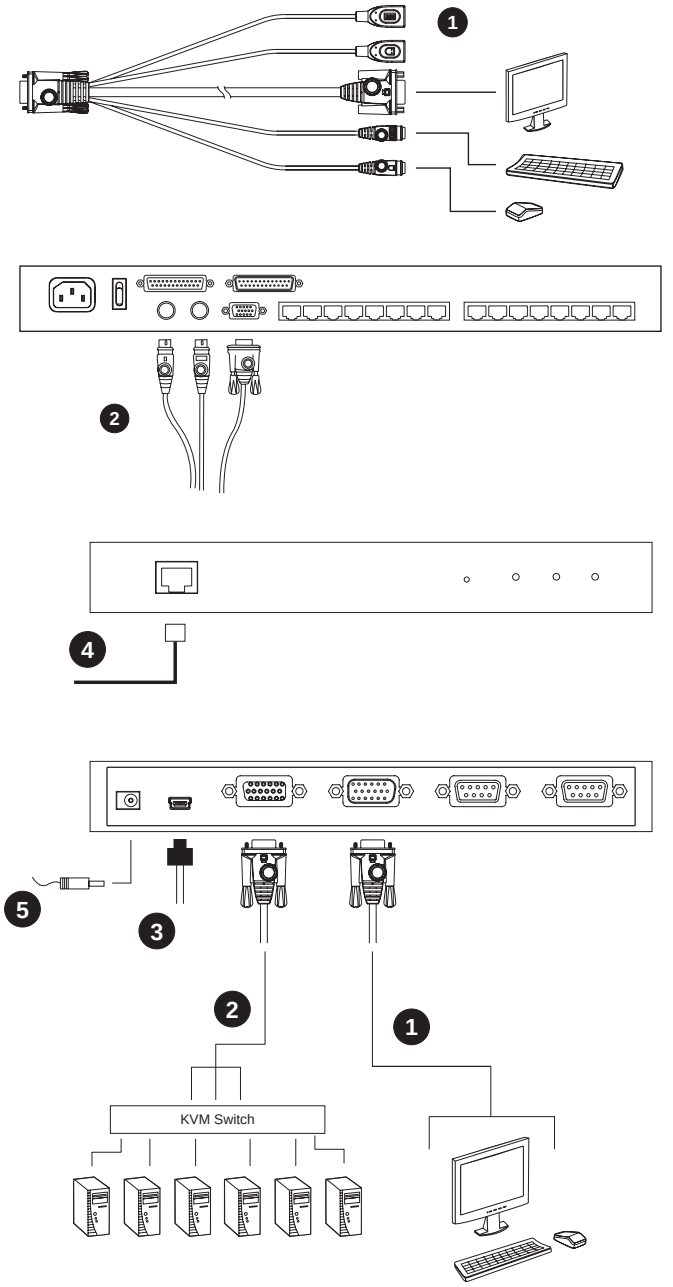
3. Hang the unit on the DIN rail.

Hardware Setup

Installation

To install the B051-000, refer to both the installation diagrams and the following steps:

1. To add a local console, connect the included USB – PS/2 Console connector kit to the B051-000 Console port. Connect the local keyboard, monitor and mouse to the connector ports on the USB – PS/2 Console connector kit. Note: You can use any combination of keyboard and mouse connections. For example, you can use a PS/2 keyboard with a USB mouse.
2. The B051-000 comes with both a PS/2 and a USB KVM cable kit, allowing you to connect to a KVM switch or server with either type of connector. Connect the Yellow HD15 connector of the included PS/2 or USB KVM cable kit to the B051-000 PC/KVM port. Plug the connectors on the other end of the KVM cable kit into the keyboard, video and mouse ports of the server or KVM switch that you are installing. Note: The diagram shows a connection to a KVM switch with PS/2 mouse and keyboard ports using a PS/2 KVM cable kit.
3. If you want to use the Virtual Media function, plug the USB 2.0 Virtual Media Cable provided with this package from a computer/server's USB port into the B051-000 Virtual Media port. Note: Virtual Media will not work if the cable is plugged into a USB port on a KVM switch that is used for keyboard/mouse functionality, it must be connected to a computer/server or a KVM USB port that is strictly a Hub port.
4. Plug a Tripp Lite Cat5e (N001- or N002-Series) or Cat6 (N201-Series) cable into the B051-000 LAN port and then connect the other end to your network jack.
5. Plug the power adapter cable into the B051-000 power jack, and then plug the power adapter into an AC power source. Note: It is recommended that you plug the unit into a Tripp Lite Surge Suppressor, UPS or Line Conditioner to help protect your system from sudden, transient increases and decreases in electrical power.



Setting up an IP Address

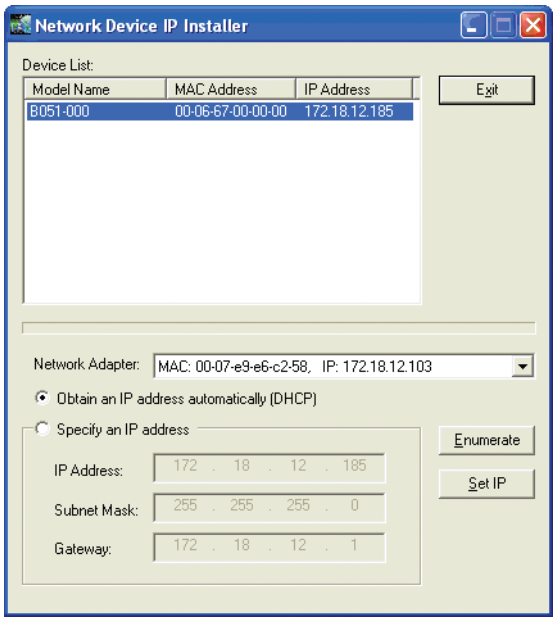
IP Address Determination

If you are an administrator logging in for the first time, you need to access the B051-000 in order to give it an IP address that users can connect to. There are three methods to choose from; IP Installer, Browser or AP Windows Client. In each case, the computer you are using to access the B051-000 must be on the same network segment as the unit. After you have connected and logged in you can give the B051-000 its fixed network address. The default username is **administrator** and the default password is **password**. It is strongly recommended that you change these upon accessing the B051-000.

IP Installer

For computers running Windows, an IP address can be assigned with the IP Installer utility:

1. Unzip the contents of IPInstaller.zip (found on the CD that came with the B051-000) and save them to a directory on your hard drive.
2. Go to the directory and run the IPInstaller.exe. A dialog box similar to the one below appears:



When the IP Installer main window comes up, the utility scans the network for B051-000 devices and lists the ones it finds in the Device List Panel. The Device List Panel consists of three columns, as shown in the following table:

Item	Description
Model Name	The device's model name (B051-000).
MAC Address	The MAC address of the device.
IP Address	The current IP Address of the device.

3. Select the B051-000 from the *Device List*.
   - If there is more than one B051-000, use the MAC address to find the unit that you want. The MAC address can be located on the bottom of the unit.
   - If the list is empty, or the B051-000 does not appear, click Enumerate to refresh the Device List.

Note: The Network Adapter drop-down list pertains to computers that have more than one network adapter installed. Users should select the network adapter that they want the Enumerate signal to be sent to.

4. Once you have selected the desired B051-000, you must choose whether you want to *Obtain an IP address automatically (DHCP)* or *Specify an IP address*. If you choose the latter, fill in the IP address, Subnet Mask, and Gateway fields with the information appropriate to your network.
5. Click **Set IP**.
6. Once the IP address shows up in the Device List, click **Exit**.

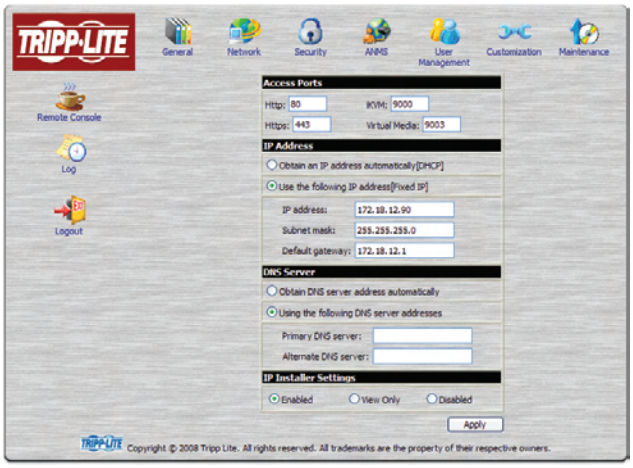
Browser

1. Set the IP address of the computer/server you are using to access the B051-000 to 192.168.0.XXX, where XXX represents any number or numbers except 10. (192.168.0.10 is the default IP address of the B051-000.)
2. Access the B051-000 by entering its default IP address (192.168.0.10) into your browser.

Setting up an IP Address

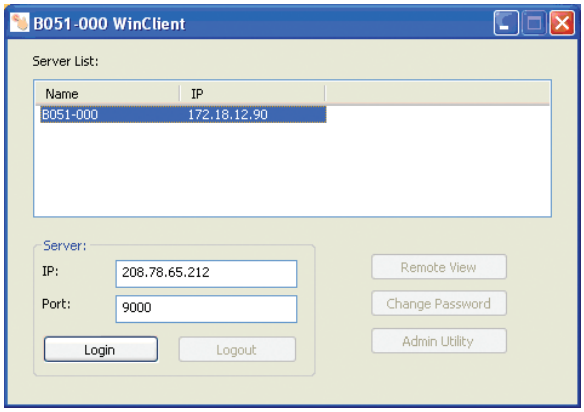
Browser *(continued)*

3. Once logged into the B051-000, you can customize the Network Settings by clicking on the Network Icon on the B051-000 home page. Assign an IP address for the B051-000 that is suitable for the network segment that it resides on.
4. After you log out, reset your computer's IP address to its original value.



AP Windows Client

For computers running Windows, the B051-000 IP address can be determined using the Windows AP program. Run the Windows Client AP Installer file from the CD that came with the B051-000 and follow the step-by-step instructions. The first time you login to the AP Windows Client, you will need the serial number located on the CD that came with the B051-000. This is not the same as the serial number on the bottom of the unit. When you run the program it searches the network segment for B051-000 devices, and displays the results in a dialog box similar to the one below:



To update the network settings, you must click on the Login button to log into the B051-000. Once logged in, click on the **Admin Utility** button to access the B051-000 Admin Utility. From there you can get to the network settings screen by clicking the **Network** tab.

Setting up an IP Address

Browser Login

The B051-000 IP Remote Access Unit can be accessed from a browser or via the Windows and/or Java application (AP) program. The next several chapters describe browser-based operations. AP access is discussed in Chapter 9.

Logging In

To login, open your browser and specify the IP address of the B051-000 you want to access in the browser's URL location bar.

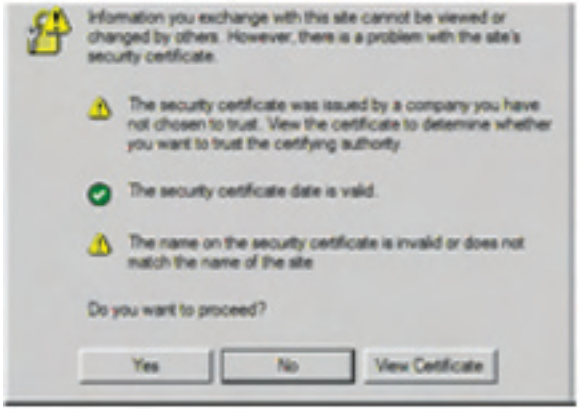
Note: If you do not know the IP address for the B051-000, ask your System Administrator.

When you try to log in to the device from your browser, a Security Alert message appears to inform you that the device's certificate is not trusted, and asks if you want to proceed.

The certificate can be trusted, but the alert is triggered because the certificate's name is not found on Microsoft's list of Trusted Authorities. You have two options:

1. Ignore the warning and click **Yes** to go on.
2. Install the certificate and have it be recognized as trusted.

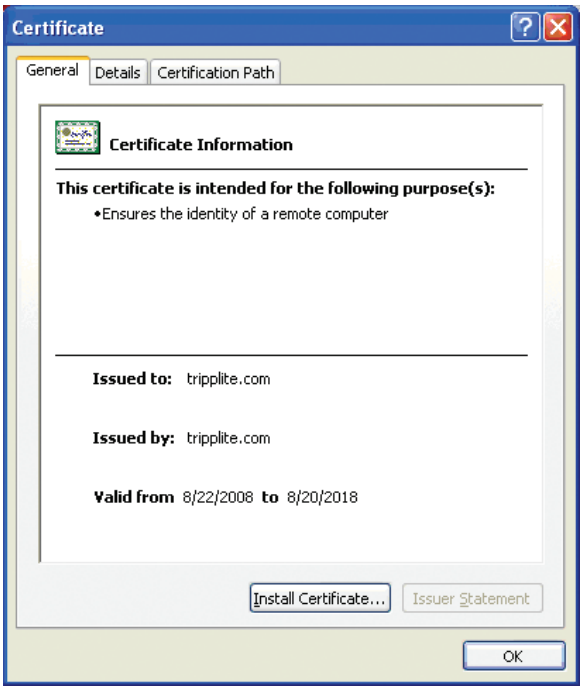
If you choose to ignore the warning and click **Yes** to login right away, skip to the text following Step 5 of the next section.



Installing the Certificate

To install the certificate, do the following:

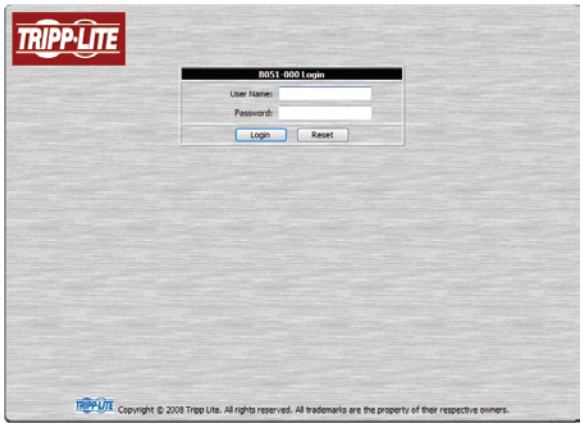
1. In the *Security Alert* dialog box, click **View Certificate**. The *Certificate Information* dialog box appears:



Note: There is a red and white **X** *logo over the certificate to indicate that it is not trusted.*

2. Click **Install Certificate**.
3. Follow the Installation Wizard to complete the installation. Unless you have a specific reason to choose otherwise, accept the default options.
4. When the Wizard presents a caution screen, click **Yes**.
5. Click **Finish** to complete the installation and click **OK** to close the dialog box. The certificate is now trusted. When you click **View Certificate**, you will see that the red and white **X** logo is no longer present.

Upon entering the URL, the B051-000 login page appears:



Provide a valid username and password and click **Login** to continue. If you do not have a username and password, contact your System Administrator.

Note: If you are the administrator, and logging in for the first time, use the default username: administrator*; and the default password:* password. *For security purposes, we strongly recommend you remove these and give yourself a unique username and password.*

Setting up an IP Address

Installing the Certificate *(continued)*

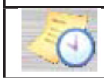
After you have successfully logged in, the B051-000 Main Screen appears:

Screen Elements

The Main Screen consists of utility icons arranged vertically down the left side of the page, administration icons arranged across the top of the page and a *Remote Console Preview* with icons to launch the Java Applet and Windows Client displayed in the center.

Note: If a user doesn't have permission to perform a particular activity, the icon for that activity doesn't appear.

Utility Icons

Icon	Function
	**Remote Console:** Clicking on this icon when on any screen will take you back to the Remote Console Preview screen.
	**Log:** All of the events that take place on the B051-000 are recorded in a log file. If you have access, clicking on this icon will allow you to view the log file.
	**Logout:** Click on this icon to logout of the B051-000. *Note: It is recommended that you logout of every session. If you exit the B051-000 without clicking the logout icon, you must wait for the logout timeout setting to expire before you can login again. (See page 27 for logout timeout setting options.)*

Administration Icons

The icons arranged horizontally across the top of the page are linked to the administration utilities, which are used to configure the B051-000. The ability to make configuration changes via these administration icons depends on the permissions associated with a user's login information. If a user does not have access to a configuration, they will not have access to its corresponding administration icon.

Note: The general *icon is non-configurable and is available to all users.*

Remote Console Preview

The main portion of the screen shows a preview of the display from the computer/server that is being accessed.

Screen Elements *(continued)*

The active elements of the Remote Console Preview are described in the following table:

Icon	Function
Refresh	Clicking **Refresh** updates the preview of the remote display.
Open Windows Client	Clicking the Open Windows Client icon will use a Windows plug-in to access the remote display on your desktop. *Note: You must be running a Windows operating system to use the Windows Client.*
Open Java Applet	Clicking the Open Java Applet icon will use a Java applet to open the remote display on your desktop. *Note: To use the Java Applet, you must have Sun's Java Runtime Environment (JRE) 6, Update 3 or higher installed on your computer.*

Note: If a user does not have permission to access the Java Applet or Windows Client, the icon will not be available on their screen. B051-000 operation using the Windows Client is discussed in Chapter 5, and operation using the Java Applet is discussed in Chapter 6.

Administration

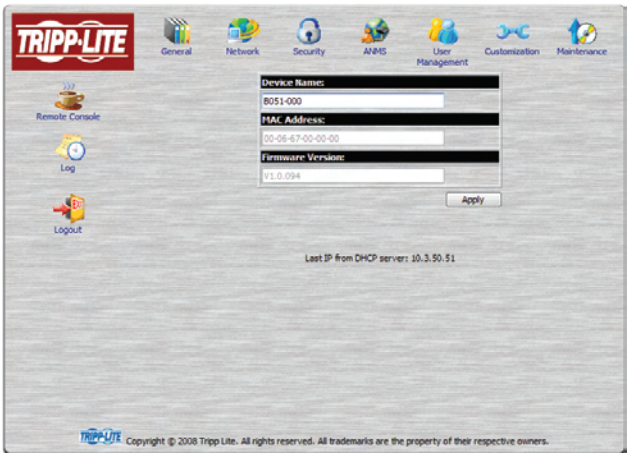
The administration utilities, represented by the icons located across the top of the B051-000 web page, are used to configure the B051-000's operating environment.

This chapter discusses each of them in turn.

Note: As you make your configuration changes in each dialog box, click ***Apply*** *to save them. After you have made all your configuration changes, in order for them to take effect, you have to put a check in the Reset on Exit box (see* Customization*, page 26), and log out. If you don't have configuration privileges, the administration icons will not be available.*

General

General page is the first of the administration icons, and provides information about the B051-000's status.

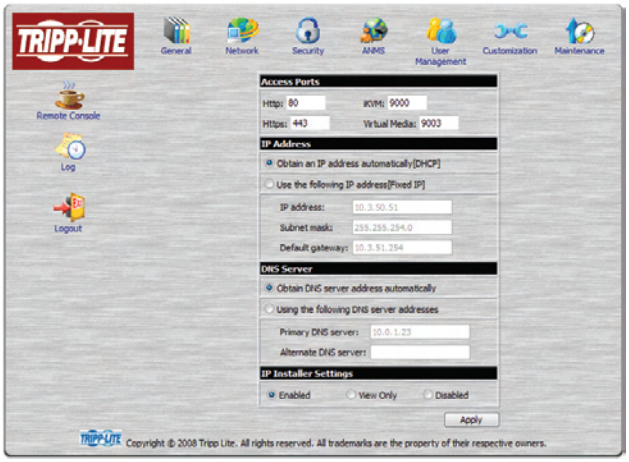


An explanation of each of the fields is given in the table below:

Field	Explanation
Device Name	To make it easier to manage installations that have more than one B051-000, each one can be given a name. To assign a name for the B051-000, type the desired name in this field (16 characters max).
MAC Address	The B051-000's MAC address displays here.
Firmware Version	Indicates the B051-000's current firmware version level. New versions of the B051-000's firmware can be downloaded from our website as they become available (see *Firmware Upgrade*, page 60). You can reference this number to see if there are newer versions available on the website.
Last IP from DHCP Server	If the B051-000 is on a network that uses DHCP assigned IP addresses, this item is a convenient way of ascertaining what its IP address is, in order to inform the Users which IP to use when they log in. *Note: If the switch has a fixed IP address, this field will not appear.*

Network

The network administration icon is used to specify the B051-000's network environment.



Administration

Access Ports

If a firewall is being used, the Administrator can specify the port numbers that the firewall will allow (and set the firewall accordingly). Users must specify the port number as part of the IP address when they connect to the B051-000. If an invalid port number (or no port number) is specified, the B051-000 will not be found. An explanation of the fields in the *Access Port* section is given in the table below:

Field	Explanation
iKVM	This is the port number that must be specified when connecting to the B051-000 from the stand-alone AP Windows Client program. Valid entries are from 1024–65535. The default is 9000.
Virtual Media	This is the port number used for data transfer when accessing the B051-000's Virtual Media feature. Valid entries are from 1024–65535. The default is 9003.
HTTP	The port number for a browser login. Valid entries are from 1–65535. The default is 80.
HTTPs	The port number for a secure browser login. Valid entries are from 1–65535. The default is 443.

Note: If there is no firewall (on an Intranet, for example), it doesn't matter what these numbers are set to, since they have no effect. The access ports cannot have the same value. You must set a different value for each one.

IP Address

The B051-000 can either have its IP address assigned dynamically when starting up (DHCP), or it can be given a fixed IP address.

- To have an IP address assigned automatically by a DHCP server, select the *Obtain an IP address automatically* button.

Note: If the B051-000 is on a network that uses DHCP to assign network addresses, and you need to ascertain its IP address, contact your system administrator.

- To specify a fixed IP address, select the *Set IP address manually* button and fill in the IP address, Subnet Mask and Default Gateway that are appropriate for your network.

DNS Server

The B051-000 can either have its DNS server address assigned automatically, or a fixed address can be specified.

- To assign a DNS server address automatically, select the *Obtain DNS server address automatically* button.
- To specify a fixed address, select the *Use the following DNS server address* button and fill in the required information.

IP Installer Settings

An IP Installer utility (IPInstaller.exe) is provided on the CD that comes with the B051-000 IP Remote Access Unit. It offers a simple method to ascertain and configure IP related settings for the B051-000. When the IP Installer is invoked, it scans the network for B051-000 devices and displays the ones it finds.

- Selecting *Enabled* allows you to see the IP settings of the devices that were found, and to use the utility to set new IP addresses.
- Selecting *View Only* allows you to see the IP settings of the devices that were found, but you cannot make any changes to the settings.
- Selecting *Disabled* will prevent the B051-000 from being found by the IP Installer.

See *IP Installer*, page 10, for operation details.

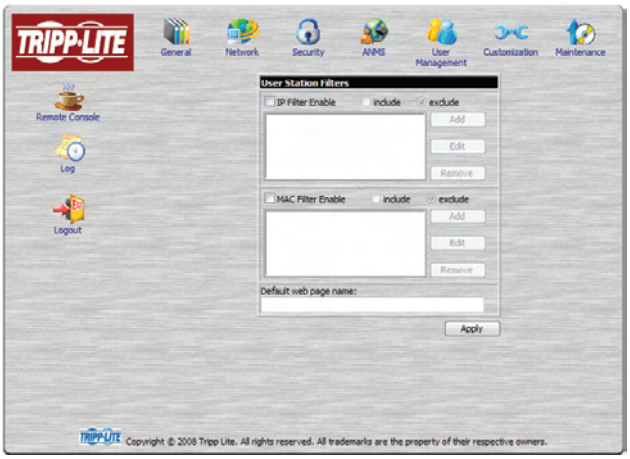
Finishing Up

After making any network changes, be sure *Reset on exit* on the *Customization* page (see *Customization*, page 26) has been enabled (there is a check in the checkbox), before logging out. This allows network changes to take effect without having to power the B051-000 off and on.

Administration

Security

The security administration icon is used to control access to the B051-000.



Overview

- *IP* and *MAC Filters* control access to the B051-000 based on the IP and/or MAC addresses of the computers attempting to access the system. If any filters have been configured, they appear in the IP Filter and/or MAC Filter list boxes.
- The *Default web page name* lets the Administrator specify a login string (in addition to the IP address) that users must include when they access the B051-000 with a browser. Users must include the forward slash and the string along when they specify the IP address in the browser's URL bar. For security purposes, we recommend that you change this string from time to time.
- **For example:** entering `abcdefg` in the *Default web page name* field will require users to type in `192.168.0.126/abcdefg` to access the B051-000 remotely.

Note: If no string is specified here, anyone can access the B051-000 with a Web browser using the IP address alone. This makes the installation less secure.

Filtering

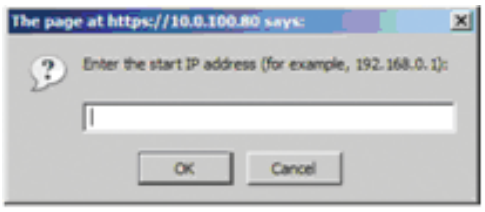
To enable IP and/or MAC filtering, click the **IP Filter Enable** and/or **MAC Filter Enable** checkbox. There are a maximum of 100 filters allowed for each.

- If the *include* button is checked, all the addresses within the filter range are allowed access to the B051-000; all other addresses are denied access.
- If the *exclude* button is checked, all the addresses within the filter range are denied access to the B051-000; all other addresses are allowed access.

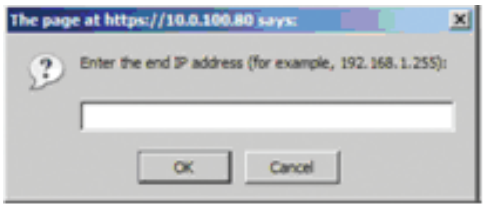
IP Filtering

To add an IP Filter:

1. Check the *IP Filter Enable* check box.
2. Click **Add**. A dialog box similar to the one below appears:



3. Type the IP address (or the first IP address in a range of IP addresses) you wish to filter in the dialog box and click **OK**. A second dialog box, similar to the one below, appears:



IP Filtering *(continued)*

4. To filter a single IP address, key in the same address as the start IP. To filter a range of addresses, key in the last IP address in the range you wish to filter.
5. After filling in the address, click **OK**.
6. Repeat these steps for any additional IP addresses you want to filter.

To delete an IP Filter:

Select the desired IP Filter from the list and click **Remove**.

To modify an IP Filter:

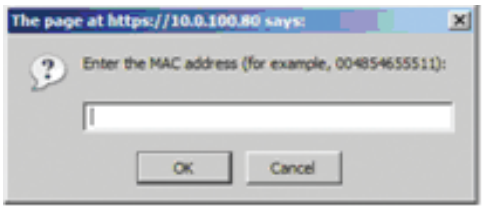
1. Select the desired IP Filter from the list and click **Edit**. An *Edit* dialog box similar to the *Add* dialog box will appear.
2. Delete the old start IP address and replace it with the new one. Click **OK**.
3. Delete the old end IP address and replace it with the new one. Click **OK**.

Note: To block a computer from accessing the B051-000, you do not need to filter both its IP address and its MAC address. Any computer blocked by an IP Filter will be denied access to the B051-000, even if the computer is allowed to access the B051-000 under the MAC Filters that are set up.

MAC Filtering

To add a MAC Filter:

1. Click **Add**. A dialog box similar to the one below appears:



2. Type in the desired MAC address and click **OK**.
3. Repeat these steps for any additional MAC addresses you want to filter.

To delete a MAC Filter:

Select the desired MAC Filter from the list and click **Remove**.

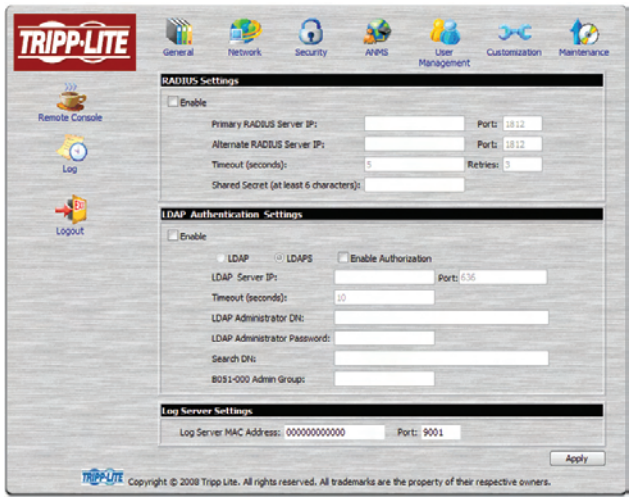
To modify a MAC Filter:

1. Select the desired MAC Filter from the list and click **Edit**. An *Edit* dialog box similar to the *Add* dialog box appears.
2. Delete the old address and replace it with the new one. Click **OK**.

Note: To block a computer from accessing the B051-000, you do not need to filter both its IP address and its MAC address. Any computer blocked by a MAC Filter will be denied access to the B051-000, even if the computer is allowed to access the B051-000 under the IP Filters that are set up.

Advanced Network Management Settings (ANMS)

The Advanced Network Management Settings (ANMS) administration icon allows you to set up login authorization management from external sources. It is divided into three main panels, as described, below:



RADIUS Settings

To allow authorization for the B051-000 through a RADIUS server, do the following:

1. Check **Enable** in the RADIUS section of the ANMS screen.
2. Fill in the IP addresses and port numbers for the Primary and Alternate RADIUS servers.
3. In the *Timeout* field, set the time in seconds that the B051-000 waits for a RADIUS server reply before it times out.
4. In the *Retries* field, set the number of allowed RADIUS retries.
5. In the *Shared Secret* field, key in the character string that you want to use for authentication between the B051-000 and the RADIUS Server.
6. On the RADIUS server, set the access rights for each user according to the information in the table below:

Character	Meaning
C	Grants the user administrator privileges, allowing the user to configure the system.
W	Allows the user to access the system via the Windows Client program.
J	Allows the user to access the system via the Java applet.
L	Allows the user to access log information via the user's browser.
V	Limits the user's access to only viewing the video display.
S	Allows the user to use the Virtual Media function.

RADIUS Server access rights examples are given in the table, below:

String	Meaning
C, W	User has administrator privileges; user can access the system via the Windows Client.
W, J, L	User can access the system via the Windows Client; user can access the system via the Java Applet; user can access log information via the user's browser.

Note: Characters are not case sensitive. Characters are comma delimited.

LDAP Authentication Settings

To allow authentication and authorization for the B051-000 via LDAPS, do the following:

Item	Description
Enable	Put a check in the *Enable* checkbox to allow LDAP / LDAPS authentication and authorization.
LDAP / LDAPS	Click to specify whether to use LDAP or LDAPS.
Enable Authorization	Click on *Enable Authorization* if you want it enabled. 1. If enabled, the LDAP / LDAPS server directly returns a 'permission' attribute and authorization for the user that is logging in. With this selection the LDAP schema must be extended. (See LDAP *Server Configuration*, page xx, for details.) 2. If not enabled, the server returns a result that depends on whether the user that is logging in belongs to the B051-000 Admin Group. If the result is 'yes' the user has full access rights (See Administrator Access Rights, page 22); if the result is 'no', the user has limited access rights. (See User Access Rights, page 22.) Note: Consult the LDAP / LDAPS administrator to ascertain whether to enable the *Enable Authorization* function, or not.
LDAP Server IP and Port	Fill in the IP address and port number for the LDAP or LDAPS server. For LDAP, the default port number is 389; for LDAPS, the default port number is 636.
Timeout	Set the time in seconds that the B051-000 waits for an LDAP or LDAPS server reply before it times out.
LDAP Administrator DN	Consult the LDAP / LDAPS administrator to ascertain the appropriate entry for this field. For example, the entry might look like this: cn=LDAPAdmin,ou=b051-000,dc=tripp lite,dc=com
LDAP Administrator Password	Key in the LDAP administrator's password.
Search DN	Set the distinguished name of the search base. This is the domain name where the search starts for user names. *Note: If* Enable Authorization *is not checked, this field must include the entry where the* B051-000 Admin Group *is created. Consult the LDAP / LDAPS administrator to ascertain the appropriate value.*
B051-000 Admin Group	Key in the Group Name for B051-000 administrators. *Note: If* Enable Authorization *is not checked, this field is used to authorize users that are logging in. If a user is in this group, the user receives full access rights. If a user is not in this group, the user only receives limited access rights. Consult the LDAP / LDAPS administrator to ascertain the appropriate value.*

LDAP Configuration

Active Directory

To allow authentication and authorization for the B051-000 via LDAP or LDAPS, the Active Directory's LDAP *Schema* must be extended so that an extended attribute name for the B051-000 – ***permission*** **–** is added as an optional attribute to the *person* class.

1. *Authentication* refers to determining the authenticity of the person logging in.
2. *Authorization* refers to assigning permission to use the device's various features.

In order to configure the LDAP server, you will have to complete the following procedures:

1. Install the Windows 2003 Support Tools.
2. Install the Active Directory Schema Snap-in.
3. Extend and Update the Active Directory Schema.

Install the Windows 2003 Support Tools

1. On your Windows Server CD, open the Support → Tools folder.
2. In the right panel of the dialog box that comes up, double click **SupTools.msi**.
3. Follow along with the Installation Wizard to complete the procedure.

Install the Active Directory Schema Snap-in

1. Open a Command Prompt.
2. Key in `regsvr32 schmmgmt.dll` to register schmmgmt.dll on your computer.
3. Open the *Start* menu. Click **Run** and key in `mmc /a`. Click **OK**.
4. On the *File* menu of the screen that appears, click **Add/Remove Snap-in**, then click **Add**.
5. Under *Available Standalone Snap-ins*, double click **Active Directory Schema**, click **Close** and click **OK**.
6. On the screen you are in, open the *File* menu and click **Save**.
7. For *Save in*, specify the *C:\Windows\system32* directory.
8. For *File name*, key in schmmgmt.msc.
9. Click **Save** to complete the procedure.

Create a Start Menu Shortcut Entry

To create a shortcut entry on the Start Menu for the Active Directory Schema, do the following:

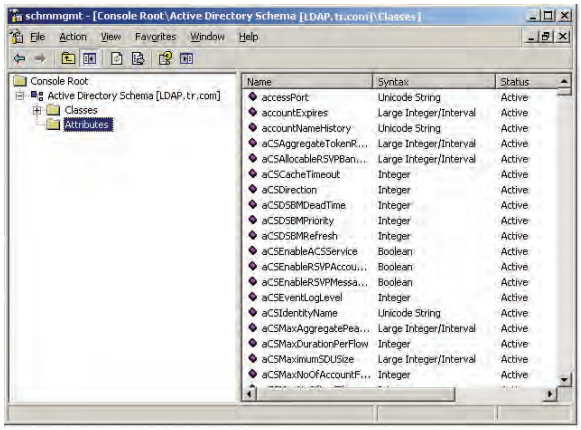
1. Right click **Start**; select: **Open all Users → Programs → Administrative Tools**.
2. On the *File* menu, select **New → Shortcut.**
3. In the dialog box that comes up, browse to or key in the path to schmmgmt.msc (C:\Windows\system32\schmmgmt.msc) and click **Next**.
4. In the dialog box that comes up, key in *Active Directory Schema* as the name for the shortcut, then click **Finish.**

Extend and Update the Active Directory Schema

Step 1 - Create a New Attribute:

a) Open **Control Panel → Administrative Tools → Active Directory Schema**.

b) In the left panel of the screen that comes up, right-click **Attributes**:

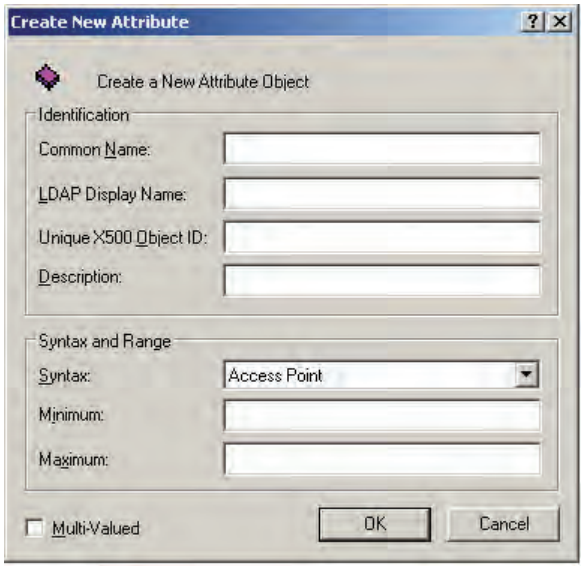


c) Select **New → Attribute**.

d) In the warning message that appears, click **Continue** to bring up the *Create New Attribute* dialog box.

e) Fill in the dialog box and click **OK** to complete Step 1 of the procedure.

Note: The Unique X500 Object ID uses periods, not commas.



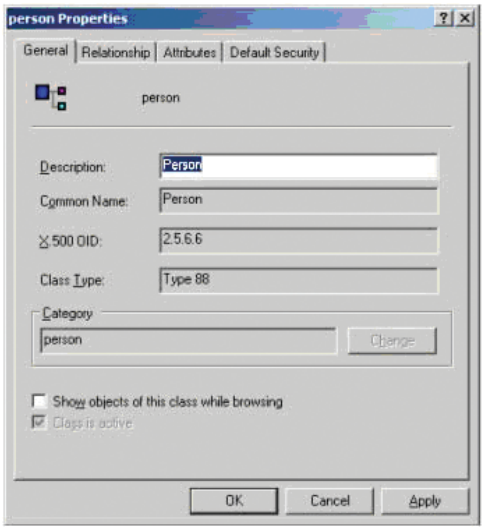
Step 2 - Extend the Object Class With the New Attribute:

a) Open **Control Panel → Administrative Tools → Active Directory Schema.**

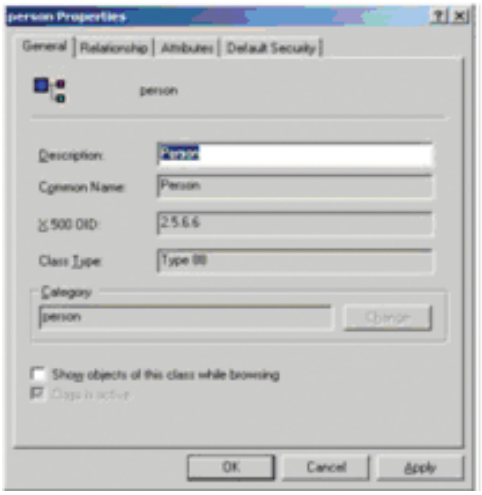
b) In the left panel of the screen that comes up, select **Classes**.

LDAP Configuration *(continued)*

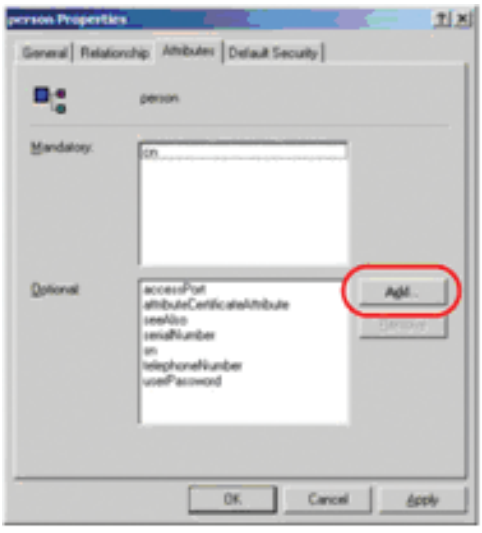
c) In the right panel, right-click **person**:



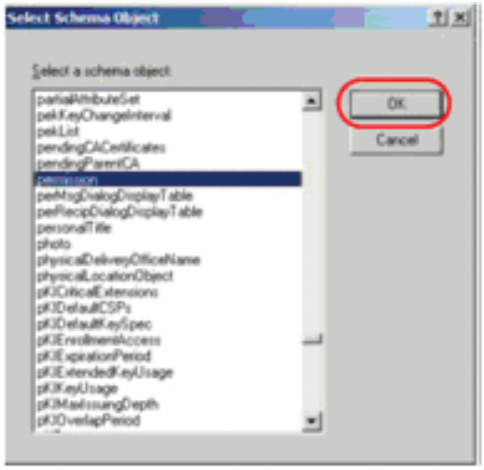
d) Select **Properties**; the person *Properties* page comes up with the *General* tab displayed. Click the *Attributes* tab.



e) Select the *Attributes* tab and click the **Add** button:



f) In the list that comes up, select **permission**, then click **OK** to complete Step 2 of the procedure.

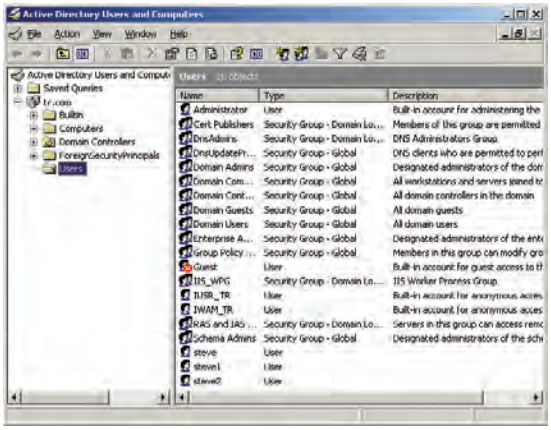


Step 3 - Edit Active Directory Users With the Extended Schema:

a) Run **ADSI Edit**. (Installed as part of the *Support Tools*.)

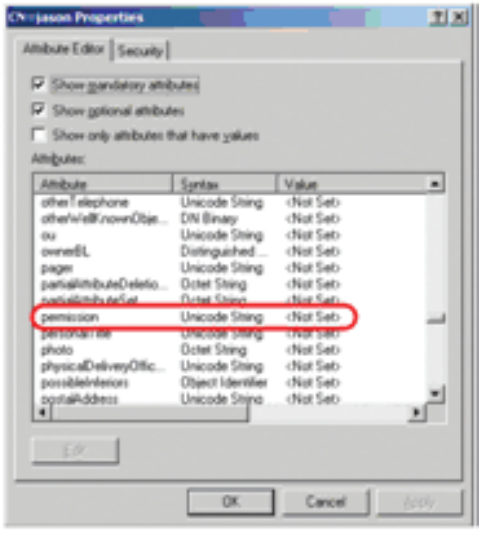
b) Open **domain**, and navigate to the *cn=users dc=tripplite dc=com* node.

c) Locate the user you wish to edit. (Our example uses *jason*.)



d) Right-click on the user's name and select **properties.**

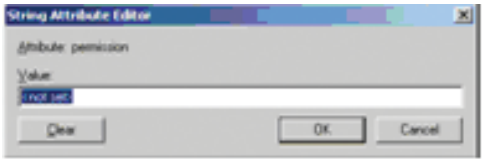
e) On the *Attribute Editor* page of the dialog box that appears, select **permission** from the list.



LDAP Configuration *(continued)*

f) Click **Edit** to bring up the *String Attribute Editor*:

g) Replace the value shown with the desired B051-000 permission attribute value. (See below for details.)



The *Permission Attribute Value* is made up of two parts; the IP address of the B051-000 a user will access and a string that indicates the access rights the user has on the B051-000 at that IP address. The following rules apply to the makeup of the permission attribute value entry:

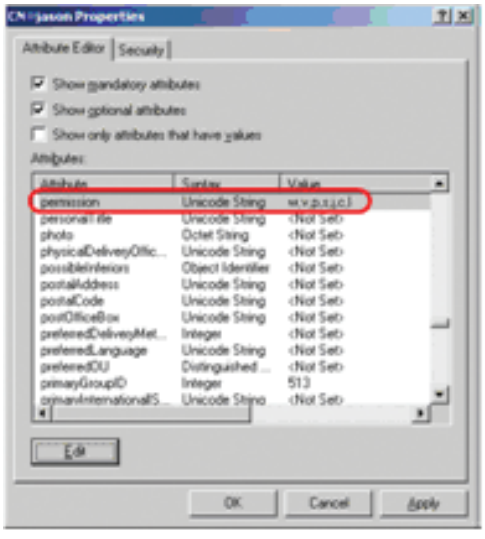
- An ampersand (&) connects the B051-000's IP address with the access rights string.
- The access rights string is made up of various combinations of the following characters: c w j l v s. The characters can be entered in upper or lower case. The meaning of the characters is provided in the *Permission String Characters* table, below.
- The characters in the access rights string are separated by a comma (,). There are no spaces before or after the comma.
- If a user has access rights to more than one B051-000, each permission segment is separated by a semicolon (;). There are no spaces before or after the semicolon.

Character	Meaning
C	Grants the user administrator privileges, allowing the user to configure the system.
W	Allows the user to access the system via the Windows Client program.
J	Allows the user to access the system via the Java applet.
L	Allows the user to access log information via the user's browser.
V	Limits the user's access to only viewing the video display.
S	Allows the user to use the Virtual Media function.

Access rights examples are given in the table below:

User	Value	Meaning
User1	10.0.0.166&w,v	1. User has Windows Client and View Only rights on a B051-000 with an IP address of 10.0.0.166. 2. User has no rights on any other B051-000 units administered by the LDAP server.
User2	10.0.0.164&s;10.0.0.166&j,c	1. User has Virtual Media rights on a B051-000 with an IP address of 10.0.0.164. 2. User has Java Applet and Administrator rights on a B051-000 with an IP address of 10.0.0.166. 3. User has no rights on any other B051-000 units administered by the LDAP server.
User3	v,l;10.0.0.164&j	1. User has View Only and Log Information rights on all B051-000 units administered by the LDAP server. 2. User has Java Applet rights on a B051-000 with an IP address of 10.0.0.164.
User4		User has no access rights to any B051-000 units administered by the LDAP server.
User5	v,w	User has View Only and Windows Client rights on all B051-000 units administered by the LDAP server.
User6	v;10.0.0.166&;10.0.0.164&c,j	1. User has View Only rights on all B051-000 units administered by the LDAP server, except for the ones with IP addresses of 10.0.0.166 and 10.0.0.164. 2. User has no access rights on the B051-000 with an IP address of 10.0.0.166. 3. User has Administrator and Java Applet rights on the B051-000 with an IP address of 10.0.0.164.

h) Click **OK**. When you return to the *Attribute Editor* page, the *permission* entry now reflects the new permissions:



i) Click **Apply** to save the change and complete the procedure.

j) Repeat Step 3 (*Edit Active Directory Users With the Extended Schema*) for any other users you wish to add.

OpenLDAP Server

OpenLDAP is an Open source LDAP server designed for UNIX platforms. A Windows version can be downloaded from:

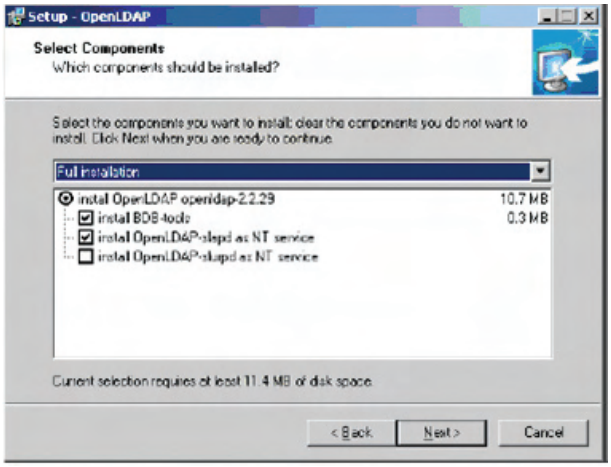
`http://download.bergmans.us/openldap/openldap-2.2.29/openldap-2.2.29-db-4.3.29-openssl-0.9.8awin32_Setup.exe.`

OpenLDAP Server Installation

After downloading the program, launch the installer, select your language, accept the license and choose the target installation directory. The default directory is:

c:\Program Files\OpenLDAP.

When the *Select Components* dialog box appears, select *install BDB-tools* and *install OpenLDAP-slapd as NT service*, as shown in the diagram:



OpenLDAP Server Configuration

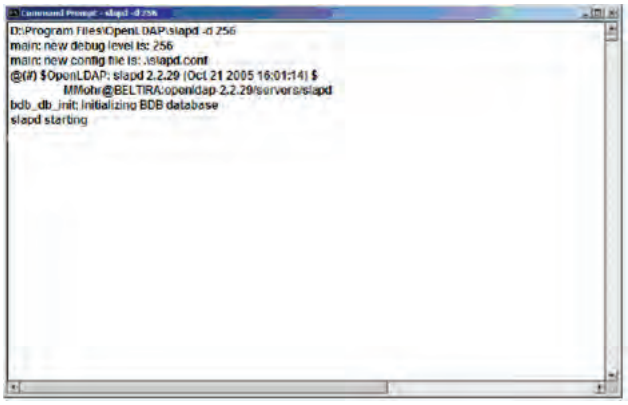
The main OpenLDAP configuration file, slapd.conf, has to be customized before launching the server. The modifications to the configuration file will do the following:

- Specify the Unicode data directory. The default is *./ucdata*.
- Choose the required LDAP schemas. The core schema is mandatory.
- Configure the path for the OpenLDAP *pid* and *args* start up files. The first contains the server pid, the second includes command line arguments.
- Choose the database type. The default is *bdb* (Berkeley DB).
- Specify the server suffix. All entries in the directory will have this suffix, which represents the root of the directory tree. For example, with suffix *dc=tripplite,dc=com*, the fully qualified name of all entries in the database will end with dc=tripplite,dc=com.
- Define the name of the administrator entry for the server (*rootdn*), along with its password (*rootpw*). This is the server's super user. The rootdn name must match the suffix defined above. (Since all entry names must end with the defined suffix, and the rootdn is an entry.)
- An example configuration file is provided in the figure, below:

```
ucdata-path ./ucdata
include ./schema/core.schema

pidfile ./run/slapd.pid
argsfile ./run/slapd.args

database bdb
suffix "dc=tripplite,dc=com"
rootdn "cn=Manager, dc=tripplite,dc=com"
rootpw secret
directory ./data
```

Starting the OpenLDAP Server

To start the OpenLDAP server, run **slapd** (the OpenLDAP server executable file) from the command line. slapd supports a number of command line options, the most important option is the **d** switch that triggers debug information. For example, a command of `slapd -d 256` would start OpenLDAP with a debug level of 256, as shown in the following screenshot:



Note: For details about slapd options and their meanings, refer to the OpenLDAP documentation.

Customizing the OpenLDAP Schema

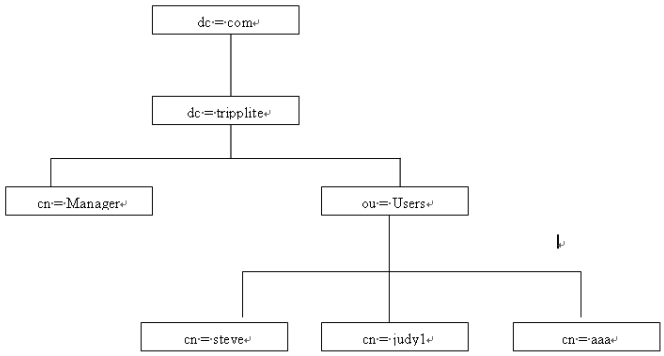
The schema that slapd uses may be extended to support additional syntaxes, matching rules, attribute types, and object classes. In the case of the B051-000, the B051-000 *User* class and the *permission* attribute are extended to define a new schema. The extended schema file used to authenticate and authorize users logging in to the B051-000 is shown in the figure, below:

```
##############################################################
##
##
##   Copyright (C) 2008 TrippLite
##   All Rights Reserved.
##   Author: Judy
##   Date:   November 27, 2008
##   Summary: Define the LDAP schema
##
##
#################################################################
#
# TRIPPLITE OID = (1.3.6.1.4.1.21317)
#


attributetype (1.3.6.1.4.1.21317.1.1.4.2.3
        NAME 'permisson'
        EQUALITY caseIgnoreMatch
        SUBSTR caseIgnoreSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
        SINGLE-VALUE)

objectclass (1.3.6.1.4.1.21317.1.1.4.1.2
        NAME 'User'
        SUP organizationalPerson
        STRUCTURAL
        MAY ('permisson'$ userCertificate)
```

LDAP DIT Design and LDIF File

LDAP Data Structure

An LDAP directory stores information in a tree structure known as the Directory Information Tree (DIT). The nodes in the tree are directory entries, and each entry contains information in attribute-value form. An example of the LDAP directory tree for the B051-000 is shown in the figure, below:



DIT Creation

The LDAP Data Interchange Format (LDIF) is used to represent LDAP entries in a simple text format (please refer to RFC 2849). The figure below illustrates an LDIF file that creates the DIT for the B051-000 directory tree (shown in the figure, above).

```
#################################################################
##
##
##   Copyright (C) 2008 TrippLite
##   All Rights Reserved.
##   Author: Judy
##   Date:   November 27, 2008
##   Summary: Define the LDAP schema
##
##
#################################################################

dn: dc=tripplite, dc=com
objectclass: top
objectClass: dcObject
objectClass: organization

dn: cn=Manager, dc=tripplite, dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: Manager
sn: Manager

dn: ou=Users, dc=tripplite, dc=com
objectclass: top
objectclass: organizationalUnit
ou: Users

dn: cn=steve,ou=Users, dc=tripplite, dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: User
cn: steve
sn: steve
permission: w,v,p,j,c,l
userPassword:password
ou: Users
```

The following figure illustrates an LDIF file that defines the OpenLDAP group for the B051-000.

```
#################################################################
##
##
##   Copyright (C) 2008 TrippLite
##   All Rights Reserved.
##   Author: Judy
##   Date:   November 27, 2008
##   Summary: Define the LDAP schema
##
##
#################################################################

dn: cn=judy1,ou=Users, dc=tripplite, dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: User
cn: judy1
sn: judy1
userPassword:password

dn: cn=ccc, dc=tripplite, dc=com
objectClass: groupOfNames
cn: ccc
member: cn=judy1, cn=users, dc=tripplite, dc=com

dn: cn=bbb, dc=tripplite, dc=com
objectClass: groupOfNames
cn: bbb
member: cn=ccc, dc=tripplite, dc=com

dn: cn=aaa, dc=tripplite, dc=com
objectClass: groupOfNames
cn: aaa
member: cn=bbb, dc=tripplite, dc=com
```

Using the New Schema

To use the new schema, do the following:

1. Save the new schema file (e.g., B051-000.schema) in the / OpenLDAP/ schema/ directory.
2. Add the new schema to the slapd.conf file, as shown in the figure, below:

```
ucdata-path     ./ucdata
include         ./schema/core.schema
include         ./schema/cosine.schema
include         ./schema/inetorgperson.schema
include         ./schema/openldap.schema
include         ./schema/.schema


# Define global ACLs to disable default read acccess.
access to dn. children="ou=Users, dc=tripplite, dc=com"
        by: dn="cn=Manager, dc=tripplite,dc=com"write
        by self read
        by anonymous auth
        by *    none


pidfile         ./run/slapd.pid
argfile         ./run/slapd.args

#######################################################
#  BDB database definitions
#######################################################

database  bdb
suffix    "dc=tripplite, dc=com"
rootdn    "cn=Manager,dc=tripplite, dc=com"
rootpw    secret
directory  ./data
```

3. Restart the LDAP server.
4. Write the LDIF file and create the database entries in init.ldif with the *ldapadd* command, as shown in the following example:

```
ldapadd -f init.ldif -x -D “cn=Manager,
dc=tripplite,dc=com” -w secret
```

Log Server Settings

Important transactions that occur on the B051-000, such as logins and internal status messages, are kept in an automatically generated log file. In order for the B051-000 to communicate with the computer that the Log Server is installed on, the *Log Server MAC Address* and *Port* fields must be filled in. (See Chapter 8 for details on setting up the log server.)

Log Server MAC Address

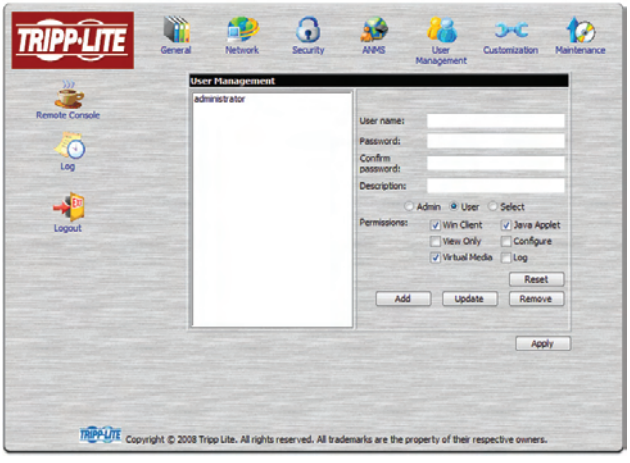
This field should contain the MAC address of the Log Server computer.

Port

This field should contain the port that the Log Server computer will use to listen for log details. The valid port range is 1024 to 65535. The default port number is 9001.

User Management

The user management administration icon is used to create and manage user profiles. Up to 64 user profiles can be established. There is no limit to the number of different user types. You can have 64 administrators, 64 users or 64 customized profiles, the only limit being you can have no more than 64 in total.



Adding a User Profile

To add a user profile, fill in the information in the right panel of the screen and click **Add**. The new user’s name appears in the User List.

Deleting a User Profile

To delete a user profile, select the desired profile from the User List and click **Remove**. The user’s name is removed from the panel.

Editing a User Profile

To edit a user profile, you must first select the desired profile from the user list. The user information will be displayed in the right panel of the screen. Edit this information and click **Update**. If you do not click the **Update** button, your changes will be lost.

Note: For security purposes, the Password *and* Confirm *fields are not displayed. If you do not want to change the user’s password, simply leave the two fields as is. If you do want to change the user’s password, key in the new password in the* Password *and the* Confirm *fields.*

User Management *(continued)*

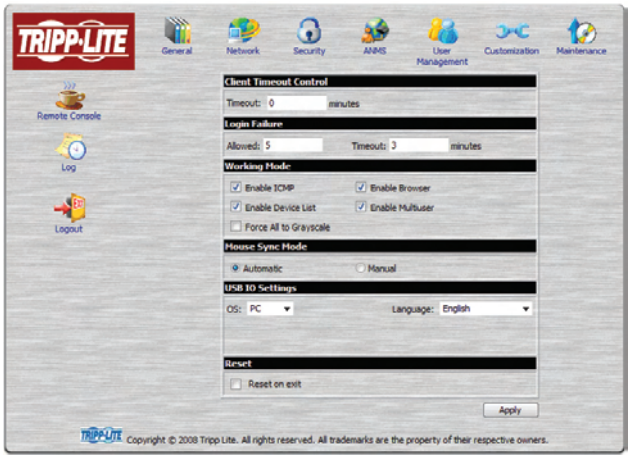
- The *Reset* button clears all the user profile information in the right panel of the screen.
- When you have made all your changes, click **Apply**. In order for your changes to be saved, the **Apply** button must be clicked. When editing a user profile, both the **Update** button and the **Apply** button must be clicked.

An explanation of the user profile items is given in the table below:

Item	Description
Username	A minimum of 6 and a maximum of 16 characters are allowed.
Password	A minimum of 6 and a maximum of 16 characters are allowed.
Confirm Password	To verify you have typed in the password correctly, you are asked to enter it again. If the two entries do not match, you will not be allowed to save the changes.
Description	This is an optional field that is used to record any additional information about the user profile.
Permissions	Click on a permission to add or remove access to a particular feature. You can choose to assign *Admin* permissions, *User* permissions or *Select* your own list of permissions. • Clicking on *Admin* will give the user access to all of the B051-000's features. The only permission box that will not be checked is the *View Only* permission. This is because *Admin* users will have full access to all computers/servers connected to the B051-000. • Clicking on *User* will give the user access to the *Win Client, Java Applet* and *Virtual Media*. They will have full access to all computers/servers connected to the B051-000. *Users* will not be able to *Configure* the B051-000 or access the *Log Server*. • Clicking on *Select* allows you to choose whatever permissions you want the user to have. When the *Admin* or *User* profiles are checked, clicking on any of the permission will automatically check the *Select* profile as well. **Win Client:** Checking *Win Client* allows a user to access the B051-000 via the Windows Client software. **View Only:** Checking *View Only* allows a user to view the video of the computers/servers connected to the B051-000, but they are not allowed to perform any operations on the computers. **Virtual Media:** Checking *Virtual Media* allows a user to utilize the B051-000's Virtual Media feature. **Java Applet:** Checking *Java Applet* allows a user to access the B051-000 via the Java Applet software. **Configure:** Checking *Configure* gives a user Administrator privileges, and allows the user to set up and modify the B051-000's operating environment. **Log:** Checking *Log* allows a user to view the contents of the log file.

Customization

The *Customization* administration icon allows the Administrator to set *Timeout, Login failure,* and *Working mode* parameters.



Customization *(continued)*

An explanation of the Customization parameters is given in the table below:

Parameter	Explanation
Timeout	If the B051-000 doesn't receive any input from a computer that is accessing it with the Windows Client or Java Applet for the amount of time specified here, it ends the connection. The default is 3 minutes.
Login Failure	**Allowed** - Sets the number of consecutive failed login attempts that are permitted from a remote computer. The default is 5. **Timeout** - Sets the amount of time a remote computer must wait before attempting to login again after it has exceeded the number of allowed failures. The default is 3 minutes.
Working Mode	**Enable ICMP** - If *ICMP* is checked, the B051-000 can be pinged, and an IP address can be assigned with the ARP command. If it is not checked, the device cannot be pinged or assigned an IP address with the ARP command. *ICMP* is checked by default. **Enable Device List** - If this item is checked, the device will show up in the list of local B051-000 units on the AP Windows Client Connection screen (see *The Windows Client Connection Screen*, page 11). If it is not checked, it will not show up. It is checked by default. **Force All to Grayscale** - If this item is checked, the remote display for all users is changed to grayscale. This can speed up I/O transfer in low bandwidth situations. By default, this item is not checked. **Enable Browser** – If this item is checked, users are allowed access to the B051-000 from a browser. If this function is not enabled, users will not be able to log into the unit via their browser. It is checked by default. **Enable Multiuser** – If this item is checked, multiple users can log into the B051-000 at the same time. It is checked by default.
Mouse Sync Mode	**Automatic** – If this item is checked, the B051-000 will automatically sync the remote and local mouse pointers. It is checked by default. *Note: This feature only supports USB mice on Windows and Mac (G4 or higher) systems. For all other configurations, we recommend that you select* Manual. **Manual** – If this item is checked, all mouse synching must be done manually with the Windows Client and Java Applet synching procedures. (See *Auto-Sync* on pages 30 and 36 for details.) By default, this item is not checked. *Note: Sun systems must use the Manual setting.*
USB IO Settings	**OS** - When connecting to a computer or KVM switch with the USB connector for keyboard and mouse, drop down the list to select the platform it uses. Choices are PC, Mac1, Mac2, and Sun. PC is the default OS. *Note: In general, Mac 1 works best with older Mac OS versions, whereas Mac 2 works best with newer ones. This may vary, however. If you encounter problems with one setting, try selecting the other one.* **Language** - When connecting to a computer or KVM switch with the USB connector for keyboard and mouse, drop down the list to select the keyboard language it uses. English is the default language.
Reset	Some configuration changes only take effect after a B051-000 reset. These include changes on the Network page, a Log Server port change, enabling/disabling browser access and upgrading the firmware. For those changes, a check is automatically put in the *Reset on Exit* box. To have the changes take effect, log out and then log back in again. A wait of approximately 30 to 60 seconds is necessary before logging in following the reset. *Note: If the B051-000's performance degrades, reset it by putting a check in the* Reset on Exit *box, and then log out / log in.*

Maintenance

The *Maintenance* page allows the Administrator to upgrade the B051-000's firmware and to backup and restore its configuration settings and user profile information.

Firmware Upgrade

As new versions of the B051-000 firmware become available, they can be downloaded from www.tripplite.com. If there are no firmware upgrade files on our website, none are currently available.

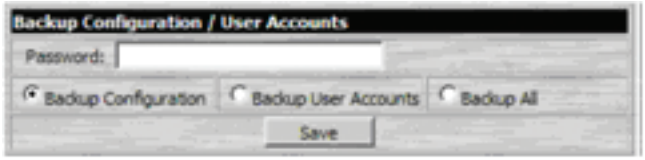
To upgrade the firmware, do the following:

1. Download the new firmware file to a computer that is on the same network as the B051-000, but not directly connected to it.
2. On the same computer, open your browser, log in to the B051-000 and click on the *Maintenance* administration icon.

3. Click the **Browse** button next to the Firmware File field, navigate to the new firmware file you just saved and select the file.
4. Click **Upload**.
5. After the upload completes, a message appears on the screen to inform you that the firmware upgrade succeeded. Click the **Logout** icon on the bottom left side of the web page.
6. In the screen that comes up click **Yes** to confirm that you want to exit and reset the B051-000. **Note:** You will need to wait between 30 and 60 seconds before logging back in.

Backup Configuration / User Accounts

The *Backup Configuration / User Accounts* section of the page gives you the ability to back up the B051-000's configuration and/or user profile information.



Maintenance *(continued)*

To perform a backup, do the following:

1. In the *Password* field, key in a password for the file. **Note:** Make a note of the password, as you will need it to be able to restore the file.
2. Select what information you want to backup. You can backup the B051-000 configuration settings, user profile information or both.
3. Click **Save**.
4. When asked what you want to do with the file, select *Save to disk*, and save it in a convenient location. **Note:** The B051-000 saves all its backup files as *B051-000BKUP.conf*. If you want to save more than one backup file, simply rename the file to something convenient when you save it.

Restore Configuration / User Accounts

Saved Configuration / User Accounts information can be restored in the *Restore Configuration / User Accounts* section of the page.

To restore a previous backup, do the following:

1. In the *Password* field, key in the same password that you used to save the file.
2. Click **Browse**. Navigate to the file and select it. **Note:** If you renamed the file, you can leave the new name. There is no need to return it to its original name.
3. Click **Restore**.

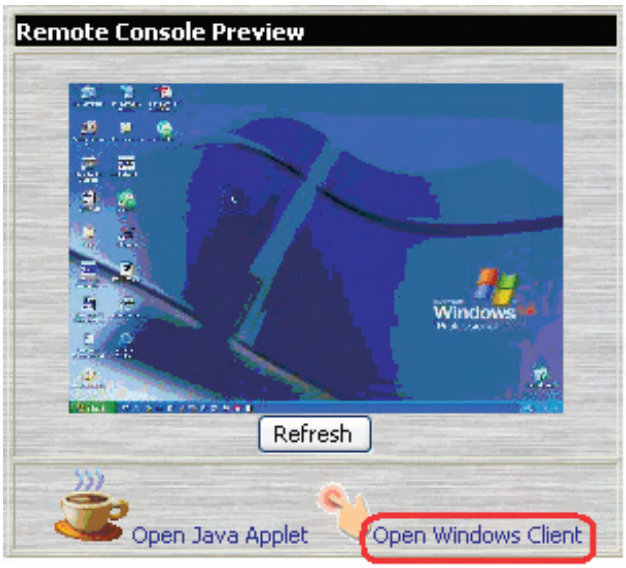
After the file is restored, a message appears to inform you that the procedure succeeded.

The Windows Client

Starting Up

To start the Windows Client, log in to the B051-000 and click the *Open Windows Client* link on the *Remote Console Preview* panel.

Note: The Windows Client will not be available when using Mozilla Firefox.



Shortly after you click the *Open Windows Client* link, the remote server's display appears as a window on your desktop:

Navigation

- You can work on the remote system just as if it were your local system.
- You can maximize the window, drag the borders to resize the window or use the scrollbars to move around the screen.
- To switch between your local and remote programs, minimize the Windows Client window and use **[Alt + Tab]** as you normally would.

Mouse Synchronization Tips

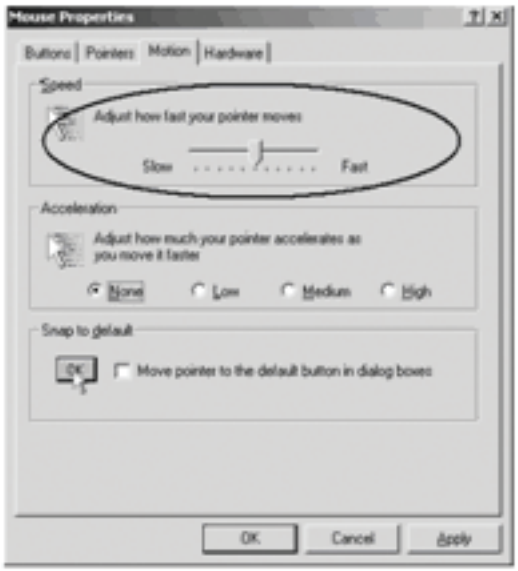
Before trying any mouse synchronization procedures, it is always a good idea to ensure that you go to your *Mouse Properties Settings* and set them according to the following:

Windows

Note: In order for the local and remote mice to synchronize, you must use the generic mouse driver supplied with the MS operating system. If you have a third party driver installed - such as one supplied by the mouse manufacturer - you must remove it.

Windows 2000:

1. Open the Mouse Properties dialog box (**Control Panel → Mouse → Mouse Properties**).
2. Click the **Motion** tab.
3. Set the mouse speed to the middle position (6 units in from the left).
4. Set the mouse acceleration to *None*.



Windows

Windows XP / Windows Server 2003:

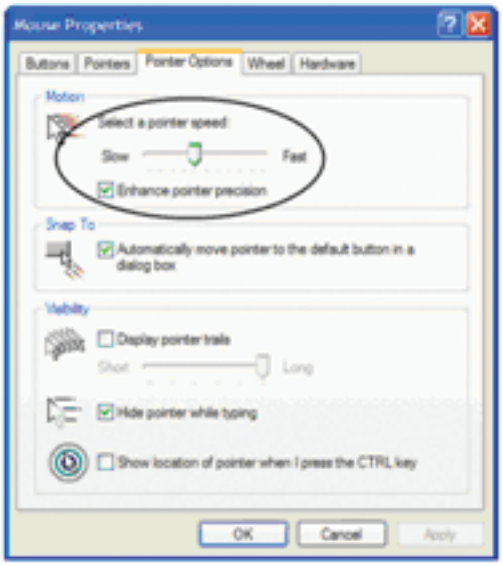
1. Open the Mouse Properties dialog box (**Control Panel → Mouse**).
2. Click the *Pointer Options* tab.
3. Set the mouse speed to the middle position (6 units in from the left).
4. Disable *Enhance Pointer Precision*.

Windows ME:

- Set the mouse speed to the middle position and disable mouse acceleration. (Click the **Advanced** button to get the dialog box for this.)

Windows NT / Windows 98 / Windows 95:

- Set the mouse speed to the slowest position.



Sun / Linux

Open a terminal session and issue the following command:

Sun: `xset m 1`

Linux: `xset m 0`

Mouse Sync Mode

In the *Customization Settings* (see page 27) screen there are two mouse sync modes; *Automatic* and *Manual*.

- **Automatic** is selected as the default, and will automatically sync the remote and local mouse pointers; however, this feature only supports USB mice on Windows and Mac (G4 or higher) systems. For all other configurations, we recommend that you select *Manual*.
- When **Manual** is checked, all mouse syncing must be done manually with the syncing procedures discussed in the following sections. Sun systems must use the Manual setting.

USB IO Settings

The *Customization Settings* (see page 27) screen contains a section called *USB IO Settings*, which can have an affect on mouse functionality. When connecting to a computer or KVM switch with the USB connector for keyboard and mouse, it is necessary to access the *OS* drop-down list in this section to select the OS platform being used. Choices are PC, Mac1, Mac2, and Sun. PC is the default OS.

Note: In general, Mac 1 works best with older Mac OS versions, whereas Mac 2 works best with newer ones. This may vary, however. If you encounter problems with one setting, try selecting the other one.

Adjust Mouse Hotkey

The Windows Client Control Panel, which is discussed in the following sections, contains a Hotkey (**Alt + M** by default) that syncs the local mouse pointer with the remote mouse pointer. Simply press the (**Alt + M**) Hotkey, and the local and remote mouse pointers should sync within a few seconds.

Auto-Sync Button

In the *Video Settings Menu*, which is discussed in the following sections, there is an *Auto-Sync* button that also serves to sync the local and remote mouse pointers. In most cases, performing an *Auto-Sync* will align the two mouse pointers.

Video Quality Slider Bar

The *Video Settings Menu* also contains a slider bar that adjusts the quality of the video being displayed on the monitor. The higher the quality of the video, the more data is being passed through the network. Higher volumes of data will cause a delay in the time that it takes for your keyboard and mouse input to appear on the monitor. To decrease the quality of the video and improve response time, adjust the *Video Quality* slider bar to a lower setting.

Detect Tolerance Slider Bar

Also in the *Video Settings Menu*, the *Detect Tolerance* slider bar can be adjusted to limit the amount of information being sent through the network. If you are having problems with keyboard and mouse response time, setting the *Detect Tolerance* slider bar to high can help.

Grayscale

Another icon contained in the Windows Client Control Panel (see the following section) is the *Grayscale* icon. Clicking this icon will force the video on the monitor to be displayed in grayscale, which can reduce the amount of data traveling through the network, and improving keyboard and mouse response time.

The Windows Client

The Windows Client Control Panel

The Windows Client Control Panel located in the top-center of the screen provides utilities to help you control remote KVM operations.

The panel consists of an icon bar with a text bar below it.

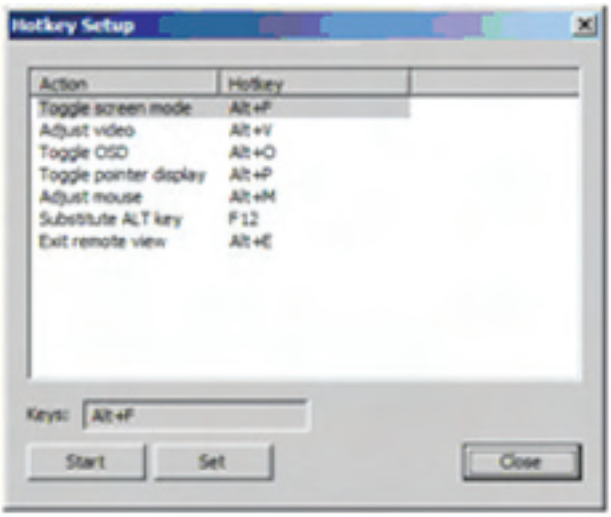
- The text bar performs two functions; it displays the remote server's video resolution, and also displays messages from the message board when you do not have the message board open. (See page 33 for more information about the message board.)
- The control panel can be moved to any location on the screen by moving the mouse pointer over one of its borders and dragging.

The icons in the control panel are described in the table below:

Icon	Description
	Click to bring up the *Hotkey Setup* dialog box.
	Click to bring up the *Video Adjustment* dialog box.
	Click to toggle the remote display between grayscale and color. Switching to grayscale can help improve the keyboard and mouse response time by decreasing the amount of data that must travel through the network connection
	Click to bring up the *Virtual Media* dialog box. The red X indicates that this feature has not been started. When in use, the icon changes to indicate the type of virtual media device being used.
	Click to open the *Message Board*.
	Click to send a *Ctrl+Alt+Del* signal to the remote system.
	Click on the keyboard to enable the on-screen keyboard. Click on the drop down arrow to bring up a list of available language keyboards. You can choose between English, Chinese (Taiwan), Japanese, German, French, Spanish, Korean and Italian.
	Click to exit the remote view.
	These icons show the **Num Lock, Caps Lock**, and **Scroll Lock** status of the remote computer. • When the lock state is *On*, the LED is bright green and the lock hasp is closed. • When the lock state is *Off*, the LED is dull green and the lock hasp is open. Click on the icon to toggle the status. *Note: When you first connect, ensure the LEDs are accurate by clicking on them to set them.*

Hotkey Setup

Various actions related to manipulating the remote server can be accomplished with hotkeys. The *Hotkey Setup* utility is accessed by clicking the icon on the Control Panel. The actions performed by the Hotkeys are listed in the left panel; the default Hotkey Commands are shown in the panel to the right.



Hotkey Setup *(continued)*

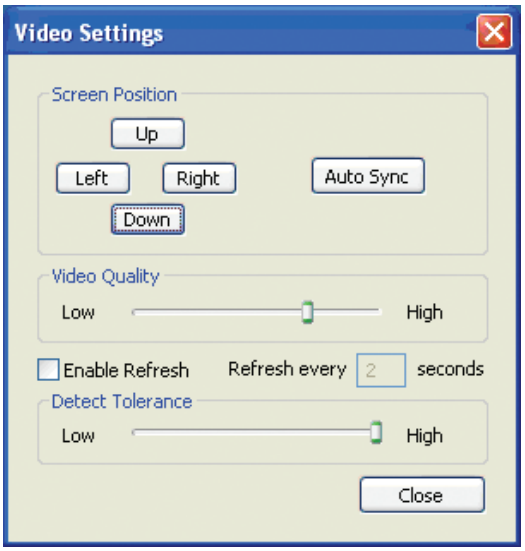
Action	Description	Default Hotkey
Toggle screen mode	Toggles the screen display between full screen and windowed modes.	Alt + F
Adjust Video	Brings up the video setting dialog box.	Alt + V
Toggle OSD	Toggles the control panel Off and On.	Alt + O
Toggle pointer display	Toggles the local mouse pointer Off and On, so you can choose to show local and remote mouse pointers at the same time, or only the remote mouse pointer.	Alt + P
Adjust Mouse	Synchronizes the movement of the local and remote mice.	Alt + M
Substitute Alt Key	Although all other keyboard input is captured and sent to the remote computer, **[Alt + Tab]** and **[Ctrl + Alt + Del]** are sent to your local computer. In order to implement their effects on the remote system, a function key is substituted for the Alt key. If you substitute the F12 key, for example, you would use **[F12 + Tab]** and **[Ctrl + F12 + Del]**.	F12
Exit remote view	Ends the remote connection to the B051-000 and returns to local operation.	Alt + E

Configuring the Hotkeys

If you find the default Hotkey combinations inconvenient, you can configure your own by following these steps:

1. Highlight the Action, then Click **Start.**
2. Key in the new combination. The key names appear in the *Key* field as you press them.
3. Click **Set.**
4. Click **Close**.

Note: Hotkey commands must be one key at a time, unless they are combined with **[Ctrl], [Alt]** *or* **[Shift]**. *In the case of combined keys, both keys must be pressed at the same time, the same as you would do when pressing* **[Ctrl] + [Alt] + [Delete]**.



Video Settings

The *Video settings* dialog box allows you to adjust the placement and picture quality of the remote screen (as displayed on your monitor).

The meanings of the adjustment options are given in the table below:

Option	Description
Screen Position	Adjust the horizontal and vertical position of the remote computer window by clicking the Arrow buttons.
Auto-Sync	Click **Auto-Sync** to have the function detect the vertical and horizontal offset values of the remote screen and automatically synchronize it with the local screen. If the local and remote mouse pointers are out of sync, in most cases, performing this function will bring them back into sync. If you are not satisfied with the results, use the Screen Position arrows to position the remote display manually. *Note: This function works best with a bright screen.*
Video Quality	Drag the slider bar to adjust the overall video quality. The higher the value, the clearer the picture and the more video data goes through the network. Depending on the network bandwidth, a high value may slow down keyboard and mouse response time.
Enable Refresh	The B051-000 can redraw the screen every 1 to 99 seconds to eliminate unwanted artifacts and provide a better picture. Select *Enable Refresh* and enter a number from 1 through 99. The B051-000 will redraw the screen at the interval you specify. This feature is disabled by default.
Detect Tolerance	This setting sets a threshold for filtering out undesired screen artifacts. Note: A high setting will decrease the amount of video information traveling through the network. If you are experiencing slow keyboard and mouse response time, this setting may help.

Grayscale

Click this button to toggle the remote display between grayscale and color. Switching to grayscale can help improve the keyboard and mouse response time by decreasing the amount of data that must travel through the network connection.

Virtual Media

The B051-000's Virtual Media feature allows a USB 2.0 device (Floppy drive, CDROM, Flash Drive, etc.), connected to a user's computer/server, to be accessible on a remote computer/server or KVM with a USB Hub port.

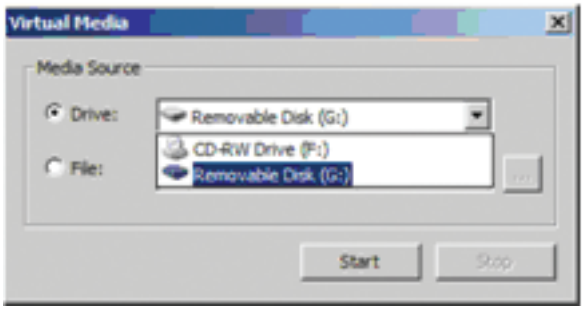
To implement this redirection feature, do the following:

Note: For the Virtual Media feature to work, the included Virtual Media USB cable must be connected between the B051-000 and the computer/server you wish to access the virtual media on. The USB cable can not be connected to a USB port on a KVM switch that is used for keyboard/mouse functionality. It can only be connected to a KVM switch that contains a USB port that is strictly a Hub port.

1. Click on the icon to bring up the *Virtual Media* dialog box:

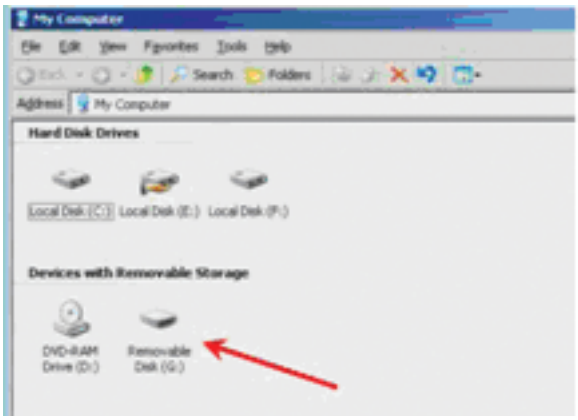
2. Select the media source.

- If you select *Drive*, drop down the drive list to select the appropriate drive:



- If you select *File*, click the button with the three dots to browse to your image file.

3. After you have made your media source selection, click **Start**. The device (or image file) that you have selected is then redirected to the remote server, where it shows up as a drive or folder on the remote server's file system.



Note: You can dismiss the Virtual Media dialog box at this point – the redirection will stay in effect. You can treat the folder as if it were really on the remote server; drag and drop files to/from it, open files on the remote system for editing and save them to the redirected drive, etc. Files that you save to the redirected drive folder will actually be saved to the USB device on your local system. Files that you drag from the redirected drive will actually come from the USB device on your local system.

4. To end the redirection, bring up the *Virtual Media* dialog box and click **Stop**.

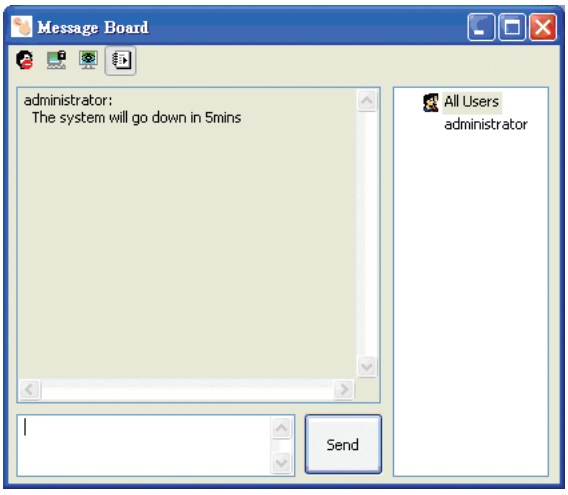
Virtual Media Icons

The Virtual Media icon on the Windows Client Control Panel changes depending on the type of drive used, as shown in the table below:

Icon	Description
	Indicates a DVD-ROM or CD-ROM drive.
	Indicates a flash (pen) drive.
	Indicates a floppy drive.

The Message Board

The B051-000 supports multiple user logins, which can possibly give rise to access conflicts. To alleviate this problem, a message board allows users to communicate with each other:



The Windows Client

The Button Bar

The buttons on the Button Bar are toggles. Their actions are described in the table below:

Button	Function
	Enable/Disable Chat - When disabled, the icon displays next to the disabled user's name in the User List panel of all users' message boards. Messages directed to the disabled user are not displayed on the message board. The button is shadowed when chat is disabled.
	Occupy/Release Keyboard/Video/Mouse - When you occupy the KVM, other users cannot see the video, and cannot input keyboard or mouse data. A prompt will come up on the locked out users' monitor stating which user has occupied the keyboard, video and mouse. The button in the message board is shadowed and the icon displays next to the occupying user's name in the User List of all users' message boards.
	Occupy/Release Keyboard/Mouse - When you occupy the keyboard and mouse, other users can see the video, but cannot input keyboard or mouse data. The button is shadowed and the icon displays next to the occupying user's name in the User List of all users' message boards.
	Show/Hide User List - When you hide the User List, the User List panel closes. The button is shadowed when the User List is open.

User List Panel

- The names of all the logged in users appear in the *User List* panel. Select the names of the users that you wish to send the message to before sending your message.
- If a user has disabled chat, its icon displays before the user's name to indicate so.
- If a user has occupied the KVM or the KM, the corresponding icon displays before the user's name to indicate so.

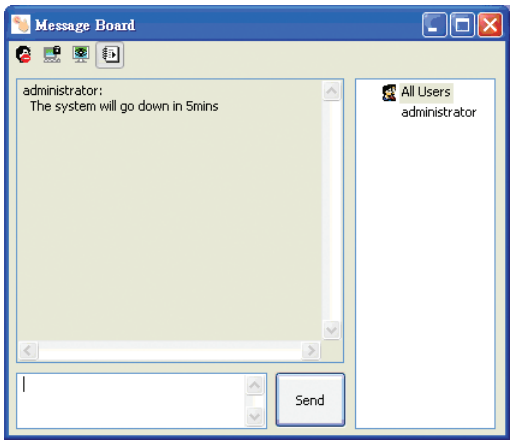
Compose Panel

Type your message into this panel. Click **Send**, or press **[Enter]** to post the message to the board.

Note: You must select the user from the user list that you want to send the message to. To send a message to all users, simply click All Users *in the user list.*

Message Display Panel

Messages that users post to the board, as well as system messages, display in this panel. If you disable chat, messages that get posted to the board will not appear.



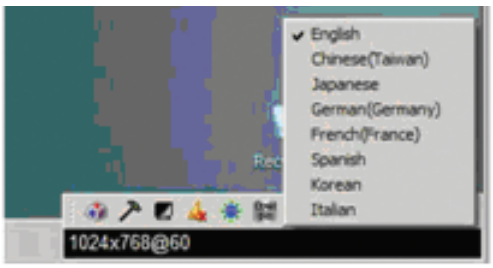
Ctrl+Alt+Del

Clicking this button sends the Ctrl+Alt+Del signal to the remote system.

On-Screen Keyboard

The B051-000 supports an on-screen keyboard, available in English, Chinese (Taiwan), Japanese, German, French, Spanish, Korean and Italian. Click on the arrow to the right of the icon to display the list of available languages:

After selecting your language, click the icon to bring up the keyboard. In the future, having selected the language, you only need to click the icon.



Exit

Click this button to exit the remote session and return to local operation.

Lock LEDs

The Lock Key LEDs show the **Num Lock, Caps Lock**, and **Scroll Lock** status of the remote computer.

- When the lock state is *Off*, the LED is dull green and the lock hasp is open.
- When the lock state is *On*, the LED turns bright green and the lock hasp is closed.

Click on the icon to toggle the status. **Note:** When you first connect, ensure the LEDs are accurate by clicking on them to set them.

The Java Applet

The Java Applet makes the B051-000 accessible to all platforms that have Java 2 installed. Java 2 is available for free download from Sun's Java web site (http://java.sun.com). To access the B051-000 with the Java Applet:

1. Log in to the B051-000 and click the *Open Java Applet* link in the *Remote Console Preview* panel.
2. After 30 seconds or so, the remote server's display appears as a window on your desktop.

Note: If a security dialog box appears, accept the certificate.

Navigation

- As with the Windows Client, you can work on the remote system just as if it were your local system.
- You can maximize the window, drag the borders to resize the window or use the scrollbars to move around the screen.
- To switch between your local and remote programs, minimize the Windows Client window and use [**Alt + Tab**] as you normally would.

Mouse Synchronization Tips

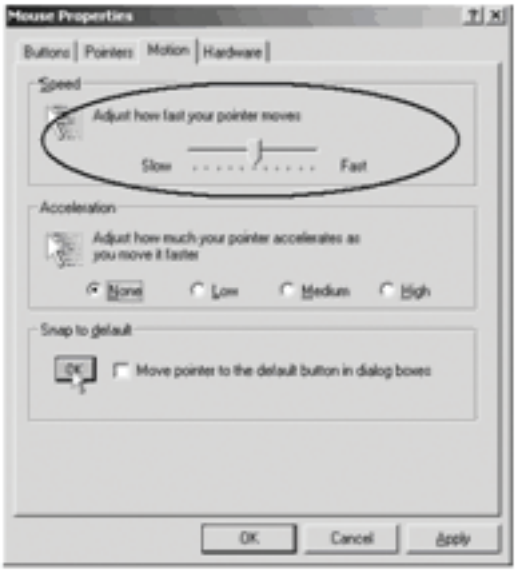
Before trying any mouse synchronization procedures, it is always a good idea to ensure that you go to your *Mouse Properties Settings* and set them according to the following:

Windows

Note: In order for the local and remote mice to synchronize, you must use the generic mouse driver supplied with the MS operating system. If you have a third party driver installed - such as one supplied by the mouse manufacturer - you must remove it.

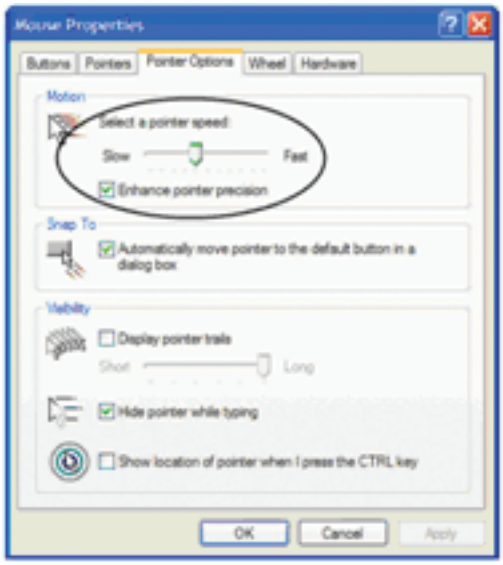
Windows 2000:

1. Open the Mouse Properties dialog box (**Control Panel → Mouse → Mouse Properties**)
2. Click the **Motion** tab.
3. Set the mouse speed to the middle position (6 units in from the left).
4. Set the mouse acceleration to *None*.



Windows XP / Windows Server 2003:

1. Open the Mouse Properties dialog box (**Control Panel → Mouse**)
2. Click the **Pointer Options** tab.
3. Set the mouse speed to the middle position (6 units in from the left).
4. Disable *Enhance Pointer Precision*.



Windows *(continued)*

Windows ME:

- Set the mouse speed to the middle position and disable mouse acceleration. (Click the **Advanced** button to get the dialog box for this.)

Windows NT / Windows 98 / Windows 95:

- Set the mouse speed to the slowest position.

Sun / Linux

Open a terminal session and issue the following command:

Sun: `xset m 1`

Linux: `xset m 0`

Mouse Sync Mode

In the *Customization Settings* screen (see page 26) there are two mouse sync modes; *Automatic* and *Manual*.

- **Automatic** is selected as the default, and will automatically sync the remote and local mouse pointers; however, this feature only supports USB mice on Windows and Mac (G4 or higher) systems. For all other configurations, we recommend that you select *Manual*.
- When **Manual** is checked, all mouse syncing must be done manually with the syncing procedures discussed in the following sections. Sun systems must use the Manual setting.

USB IO Settings

The *Customization Settings* screen (see page 27) contains a section called *USB IO Settings*, which can have an affect on mouse functionality. When connecting to a computer or KVM switch with the USB connector for keyboard and mouse, it is necessary to access the *OS* drop-down list in this section to select the OS platform being used. Choices are PC, Mac1, Mac2, and Sun. PC is the default OS.

Note: In general, Mac 1 works best with older Mac OS versions, whereas Mac 2 works best with newer ones. This may vary, however. If you encounter problems with one setting, try selecting the other one.

Adjust Mouse Hotkey

The Java Client Control Panel, which is discussed in the following sections, contains a Hotkey (**Alt + M** by default) that syncs the local mouse pointer with the remote mouse pointer. Simply press the (**Alt + M**) Hotkey and the local and remote mouse pointers should sync within a few seconds.

Auto-Sync Button

In the *Video Settings Menu*, which is discussed in the following sections, there is an *Auto-Sync* button that also server to sync the local and remote mouse pointers. In most cases, performing an *Auto-Sync* will align the two mouse pointers.

Video Quality Slider Bar

The *Video Settings Menu* also contains a slider bar that adjusts the quality of the video being displayed on the monitor. The higher the quality of the video, the more data is being passed through the network. Higher volumes of data will cause a delay in the time that it takes for your keyboard and mouse input to appear on the monitor. To decrease the quality of the video and improve response time, adjust the *Video Quality* slider bar to a lower setting.

Detect Tolerance Slider Bar

Also in the *Video Settings Menu*, the *Detect Tolerance* slider bar can be adjusted to limit the amount of information being sent through the network. If you are having problems with keyboard and mouse response time, setting the *Detect Tolerance* slider bar to high can help.

Grayscale

Another icon contained in the Java Client Control Panel (see the following section) is the *Grayscale* icon. Clicking this icon will force the video on the monitor to be displayed in grayscale, which can reduce the amount of data traveling through the network, and improving keyboard and mouse response time.

The Java Applet

The Java Applet Control Panel

The Java Applet control panel, located at the bottom right of the screen, provides utilities to help you control remote KVM operations.

The panel consists of an icon bar with a text bar below it.

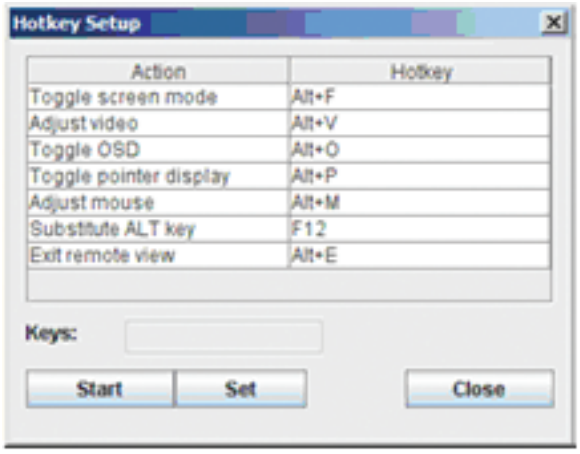
- The text bar performs two functions; it displays the remote server's video resolution, and also displays messages from the message board when you do not have the message board open. (See page 39 for more information about the message board.)
- The control panel can be moved to any location on the screen by moving the mouse pointer over one of its borders and dragging.

The icons in the control panel are described in the table below:

Icon	Description
	Click to bring up the *Hotkey setup* dialog box.
	Click to bring up the *Video settings* dialog box.
	Click to toggle the remote display between grayscale and color.
	Click to bring up the *Message board*.
	Click to send a **Ctrl+Alt+Del** signal to the remote system.
	Click on the keyboard to enable the on-screen keyboard. Click on the drop down arrow to bring up a list of available language keyboards. You can choose between English, Chinese (Taiwan), Japanese, German, French, Spanish, Korean and Italian.
	Click to exit the remote view.
	These icons show the **Num Lock, Caps Lock**, and **Scroll Lock** status of the remote computer. • When the lock state is *On*, the LED is bright green and the lock hasp is closed. • When the lock state is *Off*, the LED is dull green and the lock hasp is open. Click on the icon to toggle the status. *Note: When you first connect, ensure the LEDs are accurate by clicking on them to set them.*

Hotkey Setup

Various actions related to manipulating the remote server can be accomplished with Hotkeys. The *Hotkey Setup* utility is accessed by clicking the  icon on the Control Panel. The actions performed by the Hotkeys are listed in the left panel; the default Hotkey Commands are shown in the panel to the right.



Hotkey Setup *(continued)*

Action	Description	Default Hotkey
Toggle Screen Mode	Toggles the screen display between full screen and windowed modes.	Alt + F
Adjust Video	Brings up the video setting dialog box.	Alt + V
Toggle OSD	Toggles the control panel Off and On.	Alt + O
Toggle Pointer Display	Toggles the local mouse pointer Off and On, so you can choose to show local and remote mouse pointers at the same time, or only the remote mouse pointer.	Alt + P
Adjust Mouse	Synchronizes the movement of the local and remote mice.	Alt + M
Substitute ALT key	Although all other keyboard input is captured and sent to the remote computer, **[Alt + Tab]** and **[Ctrl + Alt + Del]** are sent to your local computer. In order to implement their effects on the remote system, a function key is substituted for the Alt key. If you substitute the F12 key, for example, you would use **[F12 + Tab]** and **[Ctrl + F12 + Del]**.	F12
Exit remote view	Ends the remote connection to the B051-000 and returns to local operation.	Alt + E

Configuring the Hotkeys

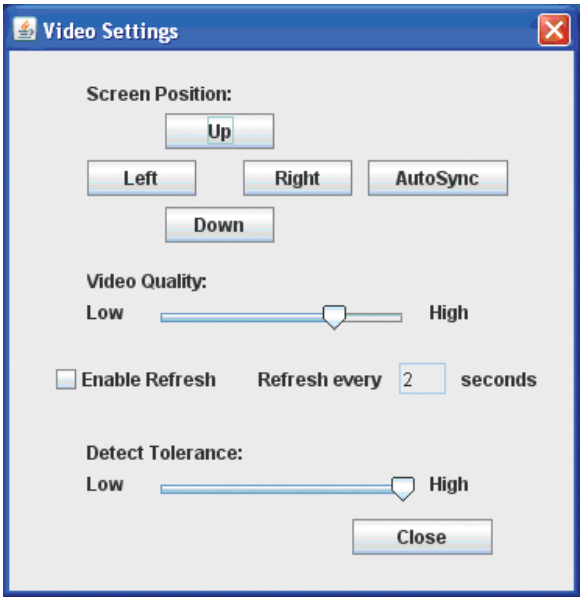
If you find the default Hotkey combinations inconvenient, you can configure your own by following these steps:

1. Highlight the Action and click **Start**.
2. Key in the new combination. The key names appear in the *Key* field as you press them.
3. Click **Set**.
4. Click **Close**.

Note: Hotkey commands must be one key at a time, unless they are combined with the **[Ctrl], [Alt]** *or* **[Shift]**. *In the case of combined keys, both keys must be pressed at the same time, the same as you would do when pressing* **[Ctrl]** + **[Alt]** + **[Delete]**.

Video Settings

The *Video settings* dialog box allows you to adjust the placement and picture quality of the remote screen (as displayed on your monitor).



Video Settings *(continued)*

The meanings of the adjustment options are given in the table below:

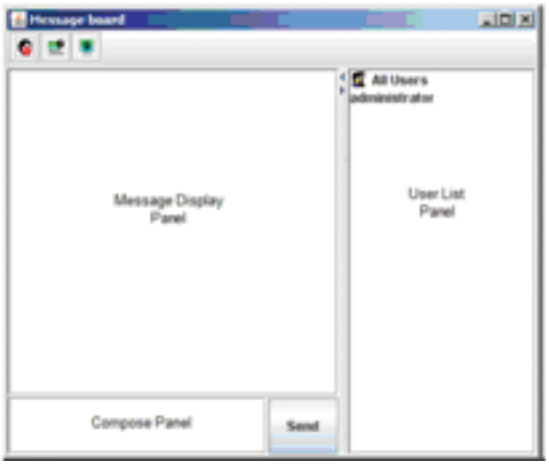
Option	Description
Screen Position	Adjust the horizontal and vertical position of the remote computer window by clicking the **Arrow** buttons.
Auto-Sync	Click **Auto-Sync** to have the function detect the vertical and horizontal offset values of the remote screen and automatically synchronize it with the local screen. If the local and remote mouse pointers are out of sync, in most cases, performing this function will bring them back into sync. If you are not satisfied with the results, use the Screen Position arrows to position the remote display manually. *Note: This function works best with a bright screen.*
Video Quality	Drag the slider bar to adjust the overall video quality. The higher the value, the clearer the picture and the more video data goes through the network. Depending on the network bandwidth, a high value may slow down keyboard and mouse response time.
Enable Refresh	The B051-000 can redraw the screen every 1 to 99 seconds to eliminate unwanted artifacts and provide a better picture. Select Enable Refresh and enter a number from 1 through 99. The B051-000 will redraw the screen at the interval you specify. This feature is disabled by default.
Detect Tolerance	This setting sets a threshold for filtering out undesired screen artifacts. *Note: A high setting will decrease the amount of video information traveling through the network. If you are experiencing slow keyboard and mouse response time, this setting may help.*

Grayscale

Click this button to toggle the remote display between grayscale and color. Switching to grayscale can help improve the keyboard and mouse response time by decreasing the amount of data that must travel through the network connection.

Message Board

The B051-000 supports multiple user logins, which can possibly give rise to access conflicts. To alleviate this problem, a message board feature, similar to an internet chat program, allows users to communicate with each other:



The buttons on the Button Bar are toggles. Their actions are described in the table below:

Button	Function
	**Enable/Disable Chat** - When disabled, the icon displays next to the disabled user's name in the User List panel of all users' message boards. Messages directed to the disabled user are not displayed on the message board. The button is shadowed when chat is disabled.
	**Occupy/Release Keyboard/Video/Mouse** - When you occupy the KVM, other users cannot see the video, and cannot input keyboard or mouse data. A prompt will come up on the locked out users' monitor stating which user has occupied the keyboard, video and mouse. The button in the message board is shadowed and the icon displays next to the occupying user's name in the User List of all users' message boards.
	**Occupy/Release Keyboard/Mouse** - When you occupy the keyboard and mouse, other users can see the video, but cannot input keyboard or mouse data. The button is shadowed and the icon displays next to the occupying user's name in the User List of all users' message boards.

User List Panel

- To Hide/Unhide the User List panel, click on the arrows in the panel separator.
- The names of all the logged in users appear in the *User List* panel. Select the names of the users that you wish to send the message to before sending your message.
- If a user has disabled chat, its icon displays before the user's name to indicate so.
- If a user has occupied the KVM or the KM, the corresponding icon displays before the user's name to indicate so.

Message Board *(continued)*

Compose Panel

Type your message into this panel. Click **Send**, or press **[Enter]** to post the message to the board.

Note: You must select the user from the user list that you want to send the message to. To send a message to all users, simply click All Users in the user list.

Message Display Panel

Messages that users post to the board, as well as system messages, display in this panel. If you disable chat, messages that get posted to the board will not appear.

Ctrl+Alt+Del

Clicking this button sends the **Ctrl+Alt+Del** signal to the remote system.

On-Screen Keyboard

The B051-000 supports an on-screen keyboard, available in English, Chinese (Taiwan), Japanese, German, French, Spanish, Korean and Italian. Click on the arrow to the right of the icon to display the list of available languages:

After selecting your language, click the icon to bring up the keyboard. In the future, after having selected the desired language, you only need to click the keyboard icon.

Exit

Click this button to exit the Java Applet and return to local operation.

Lock LEDs

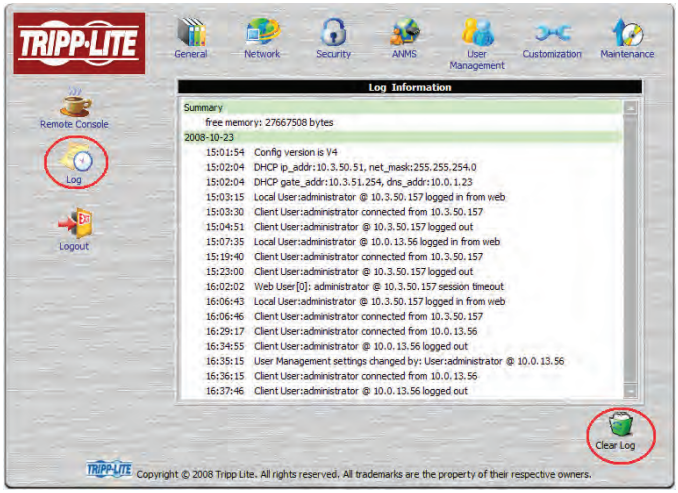
The Lock Key LEDs show the **Num Lock, Caps Lock**, and **Scroll Lock** status of the remote computer.

- When the lock state is *Off*, the LED is dull green and the lock hasp is open.
- When the lock state is *On*, the LED turns bright green and the lock hasp is closed.
- Click on the icon to toggle the status. **Note:** When you first connect, ensure the LEDs are accurate by clicking on them to set them.

The Log File

The Log File Screen

The B051-000 logs all the events that take place on it and writes them to a log file, which is a searchable database. To view the contents of the log file, click the *Log* icon at the lower left of the page. A screen similar to the one below appears:



A maximum of 512 events are kept in the log file. As new events are recorded, they are placed at the bottom of the list. When a new event is recorded after there are 512 events in the log file, the earliest event in the list is discarded. To clear the log file, click on the *Clear Log* icon at the lower right of the page.

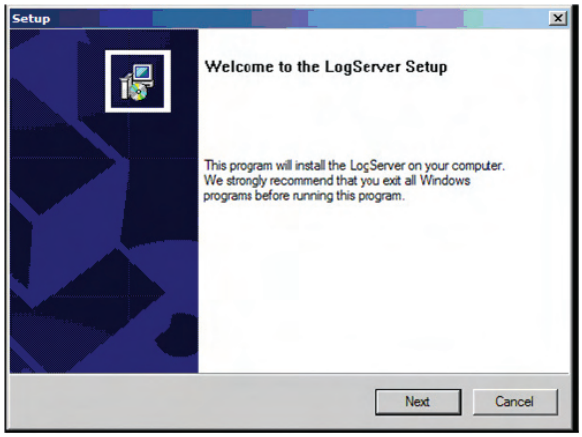
Note: To maintain and view a record of all the events that take place (not just the most recent 512), set up the Log Server AP program. (See Chapter 8, The Log Server, for details.)

The Log Server

The Windows-based Log Server is an administrative utility that records all the events that take place on selected B051-000 units and writes them to a searchable database. This chapter describes how to install and configure the Log Server.

Installation

1. From the computer that you want to use as the Log Server, open the CD that came with the B051-000 and open the Log Server Installer file.
2. If any security warning dialog boxes appear, ignore them and click **Run** or **Open**. A Log Server setup screen appears.
3. Click **Next**. Then follow the on-screen instructions to complete the installation and have the Log Server program icon placed on your desktop.
4. Before starting up the Log Server, go to the B051-000 *ANMS* settings screen and enter the MAC address and port number for the computer/server that you have installed the Log Server on. (See page 18 for details.)



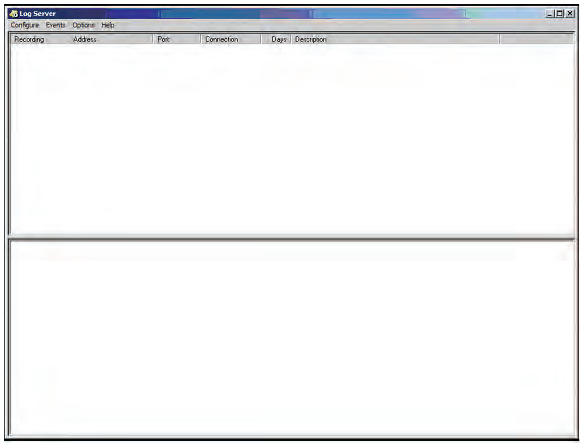
Starting Up

Double-click the Log Server icon to bring up the Log Server. The first time you run it, a screen similar to the one below appears:

Note: The Log Server requires the Microsoft Jet OLEDB 4.0 driver in order to access the database.

The screen is divided into three components:

- A *Menu Bar* at the top.
- A panel that will contain a list of all B051-000 units in the middle.
- A panel that will contain an *Events List* at the bottom.



The Menu Bar

The Menu bar consists of four drop-down menus:

- Configure.
- Events.
- Options.
- Help.

Note: If the Menu Bar appears to be disabled, select one of the B051-000 units from the list window to enable it.

Configure

The *Configure* menu consists of three functions; *Add*, *Edit* and *Delete*.

Add

Select the *Add* function when you need to add a new B051-000 to the list of units that the Log Server records events for.

Note: You must first add a B051-000 via the Add *function before the Log Server can start recording its events.*

Configure *(continued)*

When you open the *Add* function the following dialog box will appear:

Descriptions of the fields in this dialog box are shown in the table below:

Field	Description
Address	This can either be the IP address of the B051-000 or its DNS name (if the network administrator has assigned it a DNS name). This value must be entered into the *ANMS* settings screen for the B051-000 to communicate with the Log Server.
Port	Key in the port number that was specified for the B051-000 in the *ANMS* settings screen. If this differs from the port entered in the ANMS settings screen, the Log Server will not be able to communicate with the B051-000.
Description	This field is provided so that you can enter in additional information that will help differentiate this B051-000 from the rest of the B051-000 units the Log Server is recording information for.
Limit	This specifies the number of days that an event is kept in the Log Server's database before it can be deleted. To remove all events that have passed the expiration date set in this field, use the *Maintenance* function in the *Events* menu.

Edit

Select the *Edit* function when you need to change the information for an existing B051-000. To edit an existing B051-000, simply select it from the list and open the *Edit* function from the *Configure* drop-down menu. A dialog box will appear that shows the exact information that was entered for the B051-000 when it was added using the *Add* function. Edit this information and click **OK**.

Delete

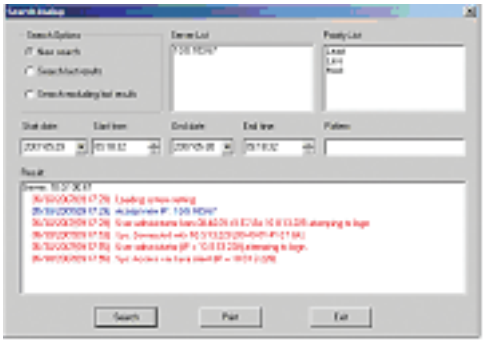
To delete a B051-000, simply select it from the list and open the *Delete* function. A dialog box will appear which will display the B051-000's information and ask you to click OK to delete it. If you want to remove it from the Log Server, click **OK**.

Events

The Events Menu consists of two items; *Search* and *Maintenance*.

Search

Search allows you to search for events containing specific words or strings. When you access this function, a screen similar to the one below appears:



Events *(continued)*

A description of the items from the *Search* screen is given in the table below:

Item	Description
Search Options	**New search:** When selected, the search is performed on all the events in the database for the selected B051-000. **Search last results:** This is a secondary search performed on the events that resulted from the last search. **Search excluding last results:** This is a secondary search performed on all the events in the database for the selected B051-000 excluding the events that resulted from the last search.
Server List	B051-000 units are listed according to their IP address. Select the unit that you want to perform the search on from this list. You can select more than one unit for the search. If no units are selected, the search is performed on all of them.
Priority List	Sets the level for how detailed the search results display should be. If nothing is selected, all results will display. If all results do display, entries highlighted in Red are of high or ***Most*** important to installations security. Entries highlighted in Blue are of medium or ***Less*** important to installtions security. Entries highlighted in Black are of the least or ***Least*** important to installations security.
Start Date	Select the date that you want the search to start from. The format follows the MM/DD/YYYY convention (e.g. 11/04/2005).
Start Time	Select the time that you want the search to start from.
End Date	Select the date that you want the search to end at. The format follows the MM/DD/YYYY convention (e.g. 11/04/2005).
End Time	Select the time that you want the search to end at.
Pattern	Key in text here that you want the search to filter the events by.
Results	The events that matched your search terms are listed here.
Search	After you have entered in all of your search terms, click this button to start the search.
Print	Click this button to print the search results.
Export	Click this button to export Log Server search results as a text file.
Exit	Click this button to exit the Search dialog box.

Maintenance

This function allows the Administrator to remove all records that have passed their expiration limit. (See page 43 for details.) In order to delete old files from the log server, the maintenance function must be performed.

Options

The *Options* menu consists of only one function; *Network Retry.*

Network Retry

Network Retry allows you to set the number of seconds that the Log Server should wait before attempting to connect in the event that the previous connection attempt failed. When you click this item, a dialog box, similar to the one below appears:

Key in the desired number of seconds and click **OK** to finish.

Help

The *Help* menu consists of two options; *Contents* and *About Log Server.*

Contents

Selecting the Contents function will bring up an online Windows Help file. The help file contains instructions about how to setup, operate and troubleshoot the Log Server.

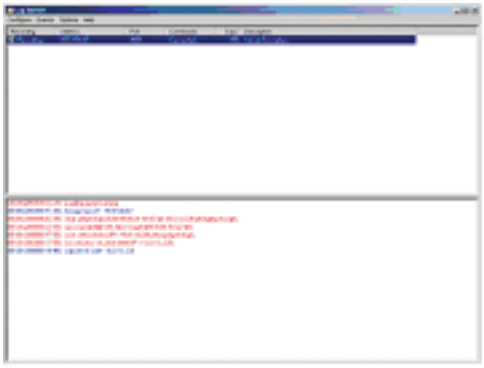
About Log Server

Selecting the *About Log Server* option will pull up a dialog box that gives you the version number of the Log Server.

The Log Server

The Log Server Main Screen

The Log Server Main Screen is divided into two main panels; an upper (List) panel that displays all of the B051-000 units that have been added to the Log Server and a lower (Event) panel that displays the log events for the currently selected B051-000. To select a B051-000 unit in the list, simply click on it.



The List Panel

The List panel contains the following fields:

Field	Description
Recording	Determines whether the Log Server records log events for the corresponding B051-000. If the Recording check box is checked, the field displays Recording, and log events are recorded. If the *Recording* check box is not checked, the field displays Paused, and log events are not recorded. *Note: Even if a B051-000 is not currently selected, if its Recording check box is checked, the Log Server will still record its log events.*
Address	This is the IP address or DNS name that was given to the B051-000 when it was added to the Log Server.
Port	This is the port number that was assigned to the B051-000 when it was added to the Log Server.
Connection	If the Log Server is connected to the B051-000, this field displays *Connected*. If it is not connected, this field displays *Waiting*. This means that the Log Server is not communicating with the B051-000, and will not record its events. This occurs when the Log Server's MAC address and/or port number have not been set properly. The MAC address and port for the Log Server computer must be entered into the B051-000's *ANMS* settings screen. In addition, the B051-000's IP address and port must be entered when adding it to the Log Server. If the port numbers in the *ANMS* menu and the Log Server do not match, the Log Server and the B051-000 will not be able to communicate.
Days	This field displays the number of days that the B051-000's log events are to be kept in the Log Server's database before it is eligible for deletion.
Description	This field displays the descriptive information given for the B051-000 when it was added to the Log Server.

The Event Panel

The lower panel displays event information for the currently selected B051-000.

AP Operation

In addition to the browser based client utilities, the B051-000 also provides stand-alone Windows and Java applications that can be used without a browser. The applications can be found on the B051-000 CD. The Windows Client program is called *B051-000winclient.exe*; the Java Client program is called *iClientJ.jar.*

Installation

To install the stand-alone Windows Client program, do the following:

1. Copy *B051-000winclient.exe* from the software CD to a convenient location on your hard disk.
2. Run the program and follow along with the installation dialog boxes. When the installation completes, an icon – *B051-000 iClient* – is placed on your desktop and a program entry is made in the Windows *Start* menu:

   (**Start → All Programs → B051-000 → iClient**).

Starting Up

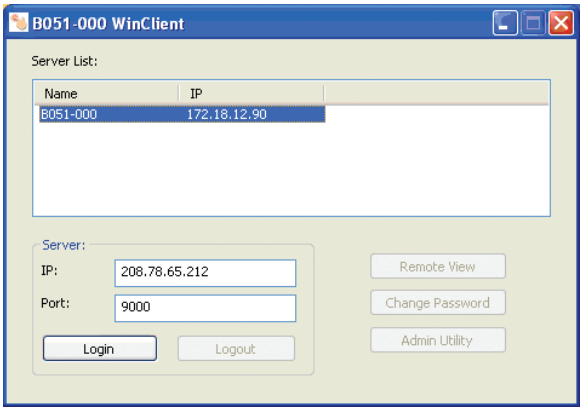
To connect to the B051-000, either click its icon on the desktop or click its entry on the Start menu.

If this is the first time that you are running the utility, a dialog box appears requesting you to input your serial number.

The serial number can be found on the B051-000's CD case. Key in the serial number (5 characters per box) and then click **OK** to bring up the B051-000 Connection Screen.

Note: This is not the same as the serial number that is on the bottom of the unit. You must use the serial number from the CD that came with the B051-000. Letters in the serial number must be entered in capitals. This dialog box only appears the first time you run the program. In the future, you go directly to the Windows Client connection screen.

The Windows Client Connection Screen



A description of the items in the AP Windows Client connection screen is given in the following table:

Item	Description
Server List	Each time the B051-000 AP Windows Client program is run, it searches the user's local LAN segment for B051-000 units, and lists whichever ones it finds in this box. If you want to connect to one of these units, select it and click Login. When you are finished with your session, click **Logout**.
Server	This area is used when you want to connect to a B051-000 at a remote location. You can drop down the *IP* list box and select an address from the list. If the address you want isn't listed, you can key in the IP address you want. Next, you will need to key in the port number in the *Port* field. If you don't know the port number, contact your System Administrator. When the IP address and port number for the unit you wish to connect to have been specified, click **Login** to start the connection. When you have finished with your session, click **Logout**.
Login	Starts the connection to the B051-000.
Logout	This button becomes active once you log into a B051-000.
Remote View	This button becomes active once you log into a B051-000.
Change Password	This button becomes active once you log into a B051-000.
Admin Utility	This button becomes active once you log into a B051-000.

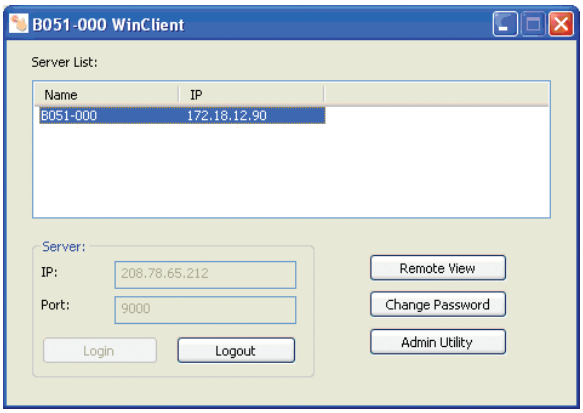
Logging In

Once the B051-000 connects to the unit you specified, a login window appears:

Provide a valid username and password and click **OK** to continue.

Note: The default username is administrator*; the default password is* password. *For security purposes, it is strongly recommended that you change these upon accessing the B051-000 for the first time.*

After you have successfully logged in, the Connection screen reappears:

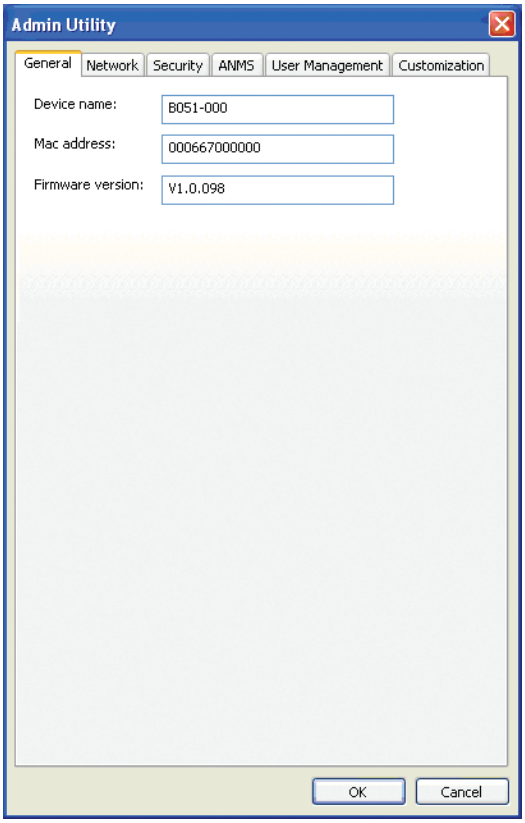


At this time there are four active buttons, as described in the table below:

Item	Description
Logout	Ends the B051-000 session.
Remote View	Click on this button to open a window on your desktop containing the remote server's display. This is the same as the one that appears with the browser-based Windows Client. (Refer to Chapter 5, The Windows Client, for operational details.)
Change Password	Allows users to change their passwords without Administrator intervention.
Admin Utility	The Administrator Utility provides administrators with a non-browser based method for configuring and controlling B051-000 operations. The Administrator Utility is discussed in the sections that follow.

The Administrator Utility

The Administrator Utility appears as a notebook with six tabs. Each tab represents a different administrative function. A description of the functions and how to configure their settings is provided in the sections that follow.



General

The Settings notebook opens with the *General* page displayed:

The Administrator Utility *(continued)*

The General page provides information about the B051-000's status, as explained in the table, below:

Item	Description
Device Name	To make it easier to manage installations that have more than one B051-000, each one can be given a name. To assign a name for the B051-000, erase the current name and key in one of your choosing (16 characters max).
MAC Address	The B051-000's MAC address displays here.
Firmware Version	Indicates the current firmware version level. New versions of the B051-000's firmware can be downloaded from our web site as they become available.

Network

This page is used to specify the B051-000's network environment.

The settings on this page are described below:

Access Ports

If a firewall is being used, the Administrator can specify the port numbers that the firewall will allow (and set the firewall accordingly). Users must specify the port number as part of the IP address when they connect to the B051-000. If an invalid port number (or no port number) is specified, the B051-000 will not be found. An explanation of the fields in the *Access Port* section is given in the table below:

Field	Explanation
iKVM	This is the port number that must be specified when connecting to the B051-000 from the stand-alone AP Windows Client program. Valid entries are from 1024–65535. The default is 9000.
Virtual Media	This is the port number used for data transfer when accessing the B051-000's Virtual Media feature. Valid entries are from 1024–65535. The default is 9003.
HTTP	The port number for a browser login. Valid entries are from 1–65535. The default is 80.
HTTPs	The port number for a secure browser login. Valid entries are from 1–65535. The default is 443.

Note: If there is no firewall (on an Intranet, for example), it doesn't matter what these numbers are set to, since they have no effect. The access ports cannot have the same value. You must set a different value for each one.

IP Installer Settings

An IP Installer utility (IPInstaller.exe) is provided on the CD that comes with the B051-000 IP Remote Access Unit. It offers a simple method to ascertain and configure IP related settings for the B051-000. When the IP Installer is invoked, it scans the network for B051-000 devices and displays the ones it finds.

- Selecting *Enabled* allows you to see the IP settings of the devices that were found, and to use the utility to set new IP addresses.
- Selecting *View Only* allows you to see the IP settings of the devices that were found, but you cannot make any changes to the settings.
- Selecting *Disabled* will prevent the B051-000 from being found by the IP Installer.

See *IP Installer*, page 10, for operation details.

IP Address

The B051-000 can either have its IP address assigned dynamically when starting up (DHCP), or it can be given a fixed IP address.

- To have an IP address assigned automatically by a DHCP server, select the *Obtain an IP address automatically* button. **Note:** If the B051-000 is on a network that uses DHCP to assign network addresses, and you need to ascertain its IP address, contact your system administrator.
- To specify a fixed IP address, select the *Set IP address manually* button and fill in the IP address, Subnet Mask and Default Gateway that are appropriate for your network.

DNS Server

The B051-000 can either have its DNS server address assigned automatically, or a fixed address can be specified.

- To assign a DNS server address automatically, select the *Obtain DNS server address automatically* button.
- To specify a fixed address, select the *Use the following DNS server address* button and fill in the required information.

Finishing Up

After making any network changes, be sure *Reset on exit* on the *Customization* page has been enabled (there is a check in the checkbox), before logging out. This allows network changes to take effect without having to power the B051-000 off and on.

Security

The Security page is used to control access to the B051-000.

The settings on this page are described below:

Overview

- *IP* and *MAC Filters* control access to the B051-000 based on the IP and/or MAC addresses of the computers attempting to access the system. If any filters have been configured, they appear in the IP Filter and/or MAC Filter list boxes.
- The *Default web page name* lets the Administrator specify a login string (in addition to the IP address) that users must include when they access the B051-000 with a browser. Users must include the forward slash and the string along when they specify the IP address. For security purposes, we recommend that you change this string from time to time. **For example:** entering `abcdefg` in the *Default web page name* field will require users to type in `192.168.0.126/abcdefg` to access the B051-000 remotely.

Note: If no string is specified here, anyone can access the B051-000 with a Web browser using the IP address alone. This makes the installation less secure.

Filtering

To enable IP and/or MAC Filtering, click the **IP Filter Enable** and/or **MAC Filter Enable** checkbox. There are a maximum of 100 filters allowed for each.

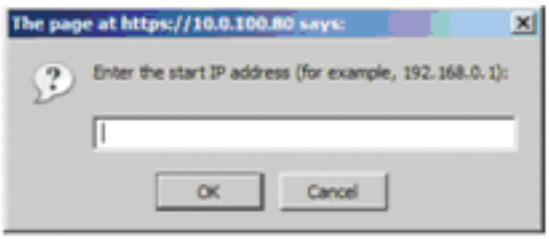
- If the *include* button is checked, all the addresses within the filter range are allowed access to the B051-000; all other addresses are denied access.
- If the *exclude* button is checked, all the addresses within the filter range are denied access to the B051-000; all other addresses are allowed access.

Filtering *(continued)*

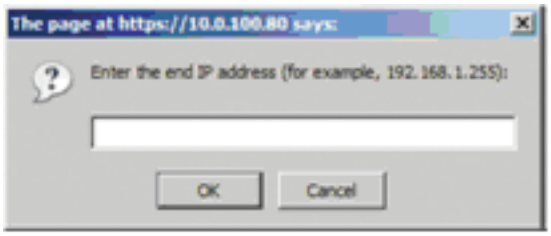
IP Filtering

To add an IP Filter:

1. Check the *IP Filter Enable* check box
2. Click **Add**. A dialog box similar to the one below appears:



3. Type the IP address (or the first IP address in a range of IP addresses) you wish to filter in the dialog box and click **OK**. A second dialog box, similar to the one below, appears:



4. To filter a single IP address, key in the same address as the start IP. To filter a range of addresses, key in the last IP address in the range you wish to filter.
5. After filling in the address, click **OK**.
6. Repeat these steps for any additional IP addresses you want to filter.

To delete an IP Filter:

Select the desired IP Filter from the list and click **Remove**.

To modify an IP Filter:

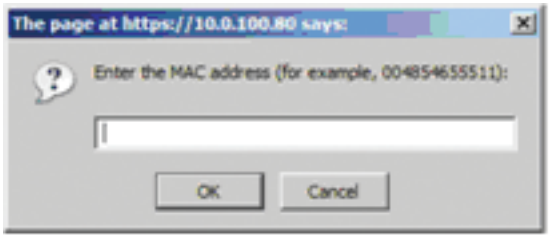
1. Select the desired IP Filter from the list and click **Edit**. An *Edit* dialog box similar to the *Add* dialog box will appear.
2. Delete the old start IP address and replace it with the new one. Click **OK**.
3. Delete the old end IP address and replace it with the new one. Click **OK**.

Note: To block a computer from accessing the B051-000, you do not need to filter both its IP address and its MAC address. Any computer blocked by an IP Filter will be denied access to the B051-000, even if the computer is allowed to access the B051-000 under the MAC Filters that are set up.

MAC Filtering

To add a MAC Filter:

1. Click **Add**. A dialog box similar to the one below appears:



2. Type in the desired MAC address and click **OK**.
3. Repeat these steps for any additional MAC addresses you want to filter.

To delete a MAC Filter:

Select the desired MAC Filter from the list and click **Remove**.

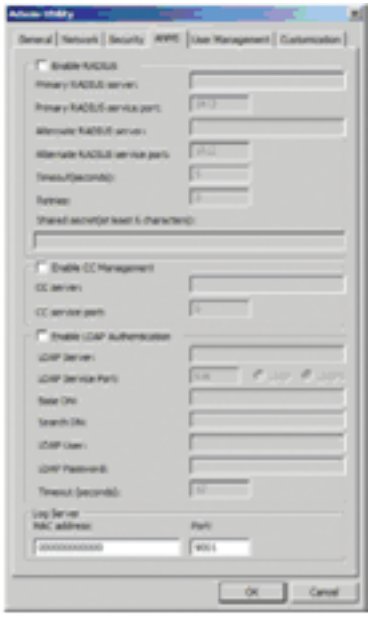
To modify a MAC Filter:

- Select the desired MAC Filter from the list and click **Edit**. An *Edit* dialog box similar to the *Add* dialog box appears.
- Delete the old address and replace it with the new one. Click **OK**.

Note: To block a computer from accessing the B051-000, you do not need to filter both its IP address and its MAC address. Any computer blocked by a MAC Filter will be denied access to the B051-000, even if the computer is allowed to access the B051-000 under the IP filters that are set up.

ANMS

The Advanced Network Management Settings dialog box allows you to set up login authorization management from an external source.



The settings on this page are described below:

RADIUS Settings

To allow authorization for the B051-000 through a RADIUS server, do the following:

1. Check **Enable** in the RADIUS section of the ANMS screen.
2. Fill in the IP addresses and port numbers for the Primary and Alternate RADIUS servers.
3. In the *Timeout* field, set the time in seconds that the B051-000 waits for a RADIUS server reply before it times out.
4. In the *Retries* field, set the number of allowed RADIUS retries.
5. In the *Shared Secret* field, key in the character string that you want to use for authentication between the B051-000 and the RADIUS Server.
6. On the RADIUS server, set the access rights for each user according to the information in the table below:

Character	Meaning
C	Grants the user administrator privileges, allowing the user to configure the system.
W	Allows the user to access the system via the Windows Client program.
J	Allows the user to access the system via the Java Applet.
L	Allows the user to access log information via the user's browser.
V	Limits the user's access to only viewing the video display.
S	Allows the user to use the Virtual Media function.

RADIUS Server access rights examples are given in the table, below:

String	Meaning
C, W	User has administrator privileges; user can access the system via the Windows Client
W, J, L	User can access the system via the Windows Client; user can access the system via the Java Applet; user can access log information via the user's browser.

Note: Characters are not case sensitive. Characters are comma delimited.

LDAP Authentication Settings

To allow authentication and authorization for the B051-000 via LDAPS, do the following:

1. Check **Enable** in the *LDAP Authentication Settings* section of the ANMS screen.
2. Select either the *LDAP* or *LDAPS* radio button.
3. Check the *Enable Authorization* check box.
4. Fill in the IP address and port number for the LDAP or LDAPS server. For LDAP, the default port number is 389; for LDAPS, the default port number is 636.
5. In the *Timeout* field: Set the time in seconds that the B051-000 waits for an LDAP or LDAPS server reply before it times out.
6. In the *LDAP Administrator DN* field, set the 'root' point for the LDAP manager to bind to the server.
7. In the *Search DN* field, set the distinguished name of the search base (i.e. the domain name where the search starts for the user name).
8. In the *B051-000 Admin Group* field, key in the name of the LDAP manager. (This field is optional.)
9. In the *LDAP Administrator Password* field, key in the LDAP manager's password. (This field is optional.)
10. On the LDAP server, set the access rights for each user. (See *LDAP Configuration* below for details on setting up LDAP for use with the B051-000.)

LDAP Configuration

Active Directory

To allow authentication and authorization for the B051-000 via LDAP or LDAPS, the Active Directory's LDAP *Schema* must be extended so that an extended attribute name for the B051-000 – ***permission –*** is added as an optional attribute to the *person* class.

- *Authentication* refers to determining the authenticity of the person logging in.
- *Authorization* refers to assigning permission to use the device's various features.

In order to configure the LDAP server, you will have to complete the following procedures: 1) Install the Windows 2003 Support Tools; 2) Install the Active Directory Schema Snap-in; and 3) Extend and Update the Active Directory Schema.

Install the Windows 2003 Support Tools

1. On the CD that came with the B051-000, open the **Support Tools** folder.
2. In the right panel of the dialog box that comes up, double click **SupTools.msi**.
3. Follow along with the Installation Wizard to complete the procedure.

Install the Active Directory Schema Snap-in

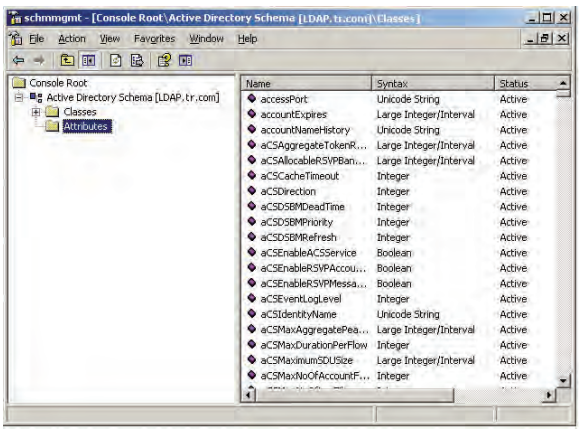
1. Open a Command prompt.
2. Key in `regsvr32 schmmgmt.dll` to register schmmgmt.dll on your computer.
3. Open the *Start* menu. Click **Run** and key in `mmc /a`. Click **OK**.
4. On the *File* menu of the screen that appears, click **Add/Remove Snap-in**, then click **Add**.
5. Under *Available Standalone Snap-ins*, double click **Active Directory Schema**, click **Close** and click **OK**.
6. On the screen you are in, open the *File* menu and click **Save**.
7. For *Save in*, specify the *C:\Windows\system32* directory.
8. For *File name*, key in schmmgmt.msc.
9. Click **Save** to complete the procedure.

Extend and Update the Active Directory Schema

Step 1 - Create a New Attribute:

a) Open Control Panel → Administrative Tools → Active Directory Schema.

b) In the left panel of the screen that comes up, right-click **Attributes**:

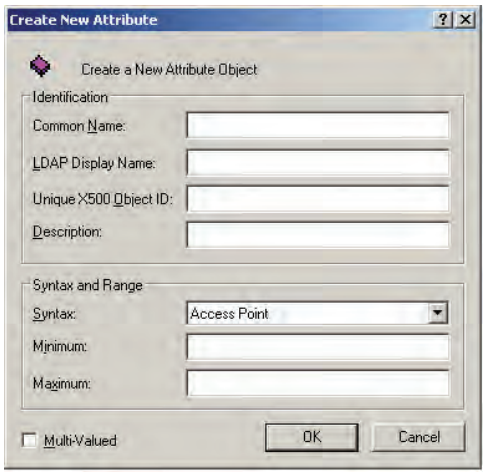


c) **Select New → Attribute**.

d) In the warning message that appears, click **Continue** to bring up the *Create New Attribute* dialog box.

e) Fill in the dialog box, then click **OK** to complete Step 1 of the procedure.

LDAP Configuration *(continued)*

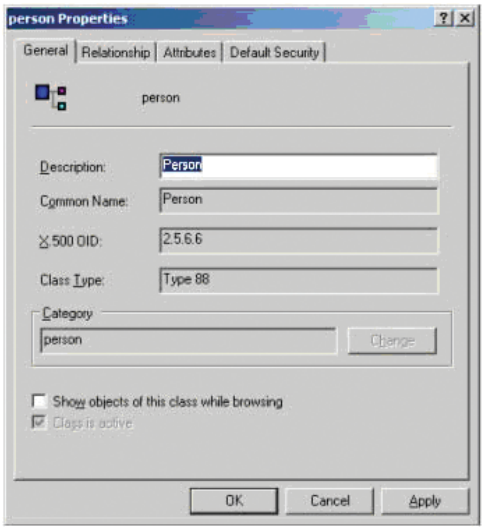


Step 2 - Extend the Object Class With the New Attribute:

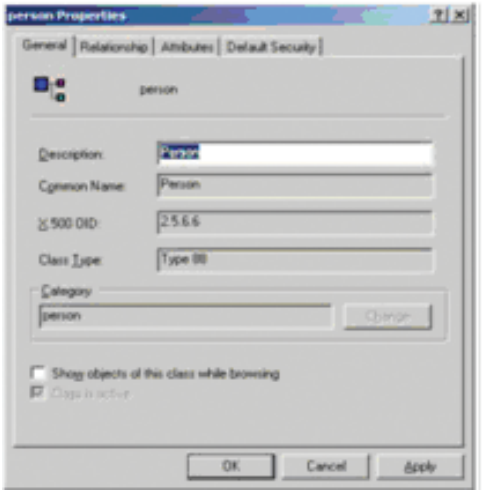
a) **Open Control Panel → Administrative Tools → Active Directory Schema**.

b) In the left panel of the screen that comes up, select **Classes**.

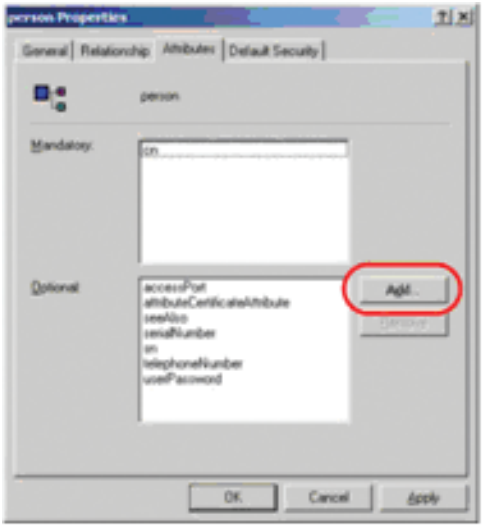
c) In the right panel, right-click **person**:



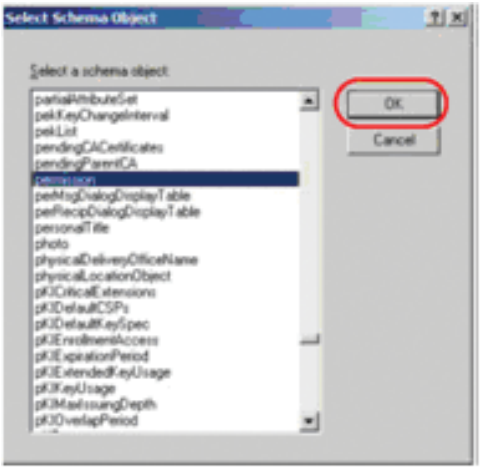
d) Select **Properties**, and fill in the *General* page of the dialog box according to the example below:



e) Select the *Attributes* tab and click the **Add** button:



f) In the list that comes up, select **permission**, then click **OK** to complete Step 2 of the procedure.

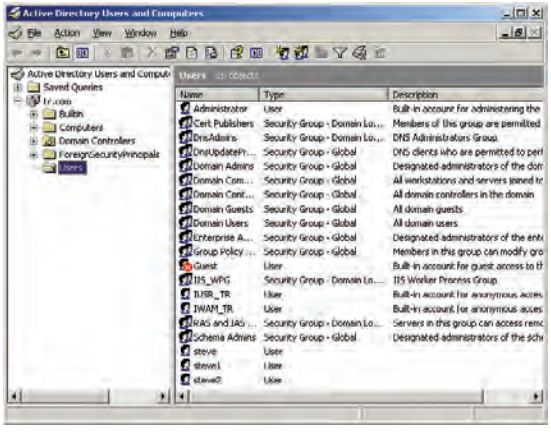


Step 3 - Edit Active Directory Users With the Extended Schema:

a) Run **ADSI Edit**. (Installed as part of the *Support Tools*.)

b) Open **domain**, and navigate to the *cn=users dc=tripplite dc=com* node.

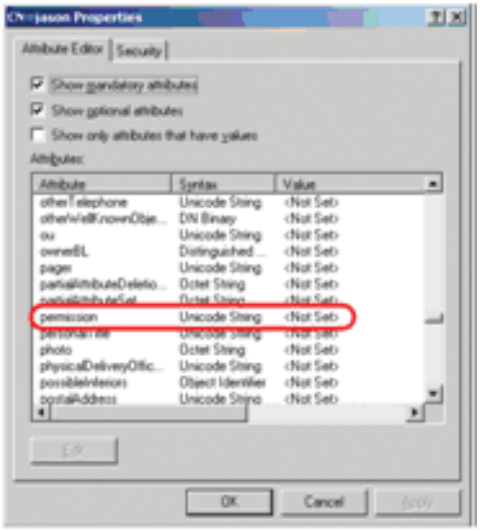
c) Locate the user you wish to edit. (Our example uses *jason*.)



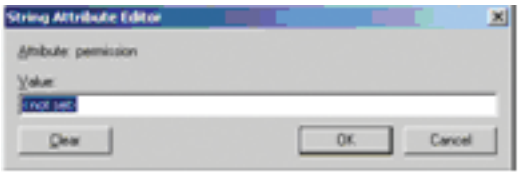
LDAP Configuration *(continued)*

d) Right-click on the user's name and select **properties.**

e) On the *Attribute Editor* page of the dialog box that appears, select **permission** from the list.



f) Click **Edit** to bring up the *String Attribute Editor*:



g) Replace the value shown with the desired B051-000 permission attribute value. (See below for details.)

The *Permission Attribute Value* is made up of two parts; the IP address of the B051-000 a user will access and a string that indicates the access rights the user has on the B051-000 at that IP address. The following rules apply to the makeup of the permission attribute value entry:

- An ampersand (&) connects the B051-000's IP address with the access rights string.
- The access rights string is made up of various combinations of the following characters: c w j l v s. The characters can be entered in upper or lower case. The meaning of the characters is provided in the *Permission String Characters* table, below.
- The characters in the access rights string are separated by a comma (,). There are no spaces before or after the comma.
- If a user has access rights to more than one B051-000, each permission segment is separated by a semicolon (;). There are no spaces before or after the semicolon.

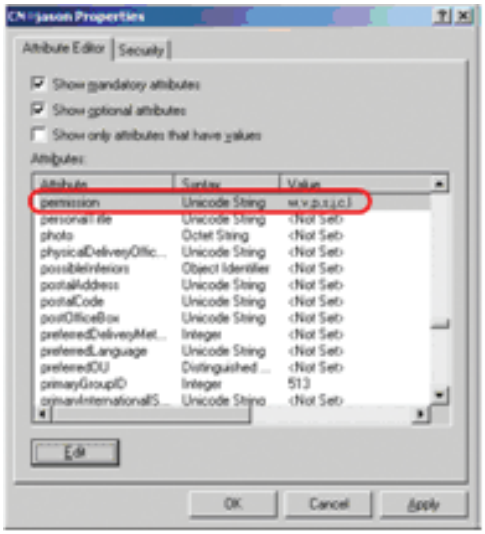
Character	Meaning
C	Grants the user administrator privileges, allowing the user to configure the system.
W	Allows the user to access the system via the Windows Client program.
J	Allows the user to access the system via the Java Applet.
L	Allows the user to access log information via the user's browser.
V	Limits the user's access to only viewing the video display.
S	Allows the user to use the Virtual Media function.

Access rights examples are given in the table below:

User	Value	Meaning
User1	10.0.0.166&w,v	1. User has *Windows Client* and *View Only* rights on a B051-000 with an IP address of 10.0.0.166. 2. User has no rights on any other B051-000 units administered by the LDAP server.
User2	10.0.0.164&s;10.0.0.166&j,c	1. User has *Virtual Media* rights on a B051-000 with an IP address of 10.0.0.164. 2. User has *Java Applet* and *Administrator* rights on a B051-000 with an IP address of 10.0.0.166. 3. User has no rights on any other B051-000 units administered by the LDAP server.
User3	v,l;10.0.0.164&j	1. User has *View Only* and *Log Information* rights on all B051-000 units administered by the LDAP server. 2. User has *Java Applet* rights on a B051-000 with an IP address of 10.0.0.164.
User4		User has no access rights to any B051-000 units administered by the LDAP server.
User5	v,w	User has *View Only* and *Windows Client* rights on all B051-000 units administered by the LDAP server.
User6	v;10.0.0.166&;10.0.0.164&c,j	1. User has *View Only* rights on all B051-000 units administered by the LDAP server, except for the ones with IP addresses of 10.0.0.166 and 10.0.0.164. 2. User has no access rights on the B051-000 with an IP address of 10.0.0.166. 3. User has *Administrator* and *Java Applet* rights on the B051-000 with an IP address of 10.0.0.164.

LDAP Configuration *(continued)*

h) Click **OK**. When you return to the *Attribute Editor* page, the *permission* entry now reflects the new permissions:



i) Click **Apply** to save the change and complete the procedure.

j) Repeat Step 3 (*Edit Active Directory Users With the Extended Schema*) for any other users you wish to add.

OpenLDAP Server

OpenLDAP is an open source LDAP server designed for UNIX platforms. A Windows version can be downloaded from:

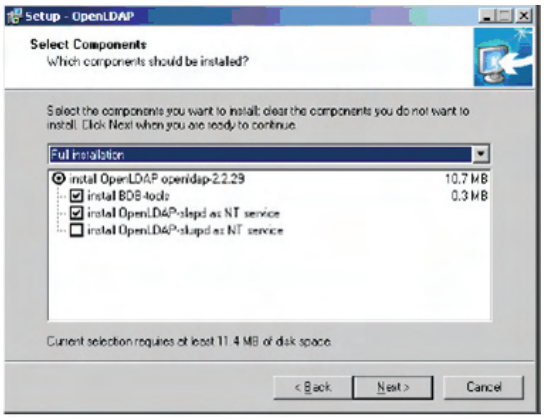
`http://download.bergmans.us/openldap/openldap-2.2.29/openldap-2.2.29-db-4.3.29-openssl-.9.8awin32_Setup.exe.`

OpenLDAP Server Installation

After downloading the program, launch the installer, select your language, accept the license and choose the target installation directory. The default directory is:

c:\Program Files\OpenLDAP.

When the *Select Components* dialog box appears, select *install BDB-tools* and *install OpenLDAP-slapd as NT service*, as shown in the diagram:



OpenLDAP Server Configuration

The main OpenLDAP configuration file, slapd.conf, has to be customized before launching the server. The modifications to the configuration file will do the following:

- Specify the Unicode data directory. The default is *./ucdata*.
- Choose the required LDAP schemas. The core schema is mandatory.
- Configure the path for the OpenLDAP *pid* and *args* start up files. The first contains the server pid, the second includes command line arguments.
- Choose the database type. The default is *bdb* (Berkeley DB).
- Specify the server suffix. All entries in the directory will have this suffix, which represents the root of the directory tree. For example, with suffix *dc=tripplite,dc=com*, the fully qualified name of all entries in the database will end with dc=tripplite,dc=com.
- Define the name of the administrator entry for the server (*rootdn*), along with its password (*rootpw*). This is the server's super user. The rootdn name must match the suffix defined above. (Since all entry names must end with the defined suffix, and the rootdn is an entry.)

OpenLDAP Server Configuration *(continued)*

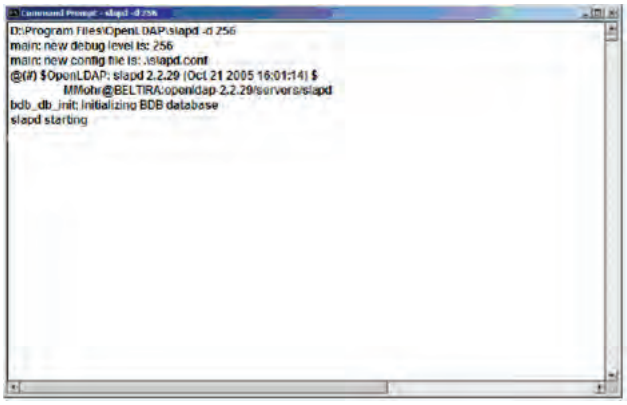
An example configuration file is provided in the figure:

```
ucdata-path ./ucdata
include ./schema/core.schema

pidfile ./run/slapd.pid
argsfile ./run/slapd.args

database bdb
suffix "dc=tripplite,dc=com"
rootdn "cn=Manager, dc=tripplite,dc=com"
rootpw secret
directory ./data
```

Starting the OpenLDAP Server

To start the OpenLDAP Server, run **slapd** (the OpenLDAP Server executable file) from the command line. **slapd** supports a number of command line options, the most important option is the **d** switch that triggers debug information. For example, a command of `slapd -d 256` would start OpenLDAP with a debug level of 256, as shown in the following screenshot:

Note: For details about slapd options and their meanings, refer to the OpenLDAP documentation.

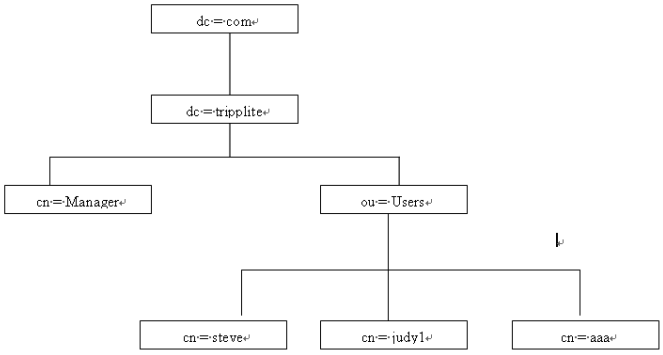


Customizing the OpenLDAP Schema

The schema that **slapd** uses may be extended to support additional syntaxes, matching rules, attribute types, and object classes. In the case of the B051-000, the B051-000*User* class and the *permission* attribute are extended to define a new schema. The extended schema file used to authenticate and authorize users logging in to the B051-000 is shown in the figure, below:

LDAP Data Structure

An LDAP directory stores information in a tree structure known as the Directory Information Tree (DIT). The nodes in the tree are directory entries, and each entry contains information in attribute-value form. An example of the LDAP directory tree for the B051-000 is shown in the figure, below:



DIT Creation

The LDAP Data Interchange Format (LDIF) is used to represent LDAP entries in a simple text format (please refer to RFC 2849). The figure below illustrates an LDIF file that creates the DIT for the B051-000 directory tree (shown in the figure, above).

```
#############################################################
##
##
##   Copyright (C) 2008 TrippLite
##   All Rights Reserved.
##   Author: Judy
##   Date:   November 27, 2008
##   Summary: Define the LDAP schema
##
##
#############################################################

dn: dc=tripplite, dc=com
objectclass: top
objectClass: dcObject
objectClass: organization

dn: cn=Manager, dc=tripplite, dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: Manager
sn: Manager

dn: ou=Users, dc=tripplite, dc=com
objectclass: top
objectclass: organizationalUnit
ou: Users

dn: cn=steve,ou=Users, dc=tripplite, dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: User
cn: steve
sn: steve
permission: w,v,p,j,c,l
userPassword:password
ou: Users
```

The following figure illustrates an LDIF file that defines the OpenLDAP group for the B051-000.

```
#############################################################
##
##
##   Copyright (C) 2008 TrippLite
##   All Rights Reserved.
##   Author: Judy
##   Date:   November 27, 2008
##   Summary: Define the LDAP schema
##
##
#############################################################

dn: cn=judy1,ou=Users, dc=tripplite, dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: User
cn: judy1
sn: judy1
userPassword:password

dn: cn=ccc, dc=tripplite, dc=com
objectClass: groupOfNames
cn: ccc
member: cn=judy1, cn=users, dc=tripplite, dc=com

dn: cn=bbb, dc=tripplite, dc=com
objectClass: groupOfNames
cn: bbb
member: cn=ccc, dc=tripplite, dc=com

dn: cn=aaa, dc=tripplite, dc=com
objectClass: groupOfNames
cn: aaa
member: cn=bbb, dc=tripplite, dc=com
```

Using the New Schema

To use the new schema, do the following:

1. Save the new schema file (e.g., B051-000.schema) in the / OpenLDAP/ schema/ directory.
2. Add the new schema to the slapd.conf file, as shown in the figure, below:

```
ucdata-path         ./ucdata
include             ./schema/core.schema
include             ./schema/cosine.schema
include             ./schema/inetorgperson.schema
include             ./schema/openldap.schema
include             ./schema/.schema


# Define global ACLs to disable default read acccess.
access to dn. children="ou=Users, dc=tripplite, dc=com"
            by: dn="cn=Manager, dc=tripplite,dc=com"write
            by self read
            by anonymous auth
            by *        none


pidfile             ./run/slapd.pid
argfile             ./run/slapd.args

#######################################################
#  BDB database definitions
#######################################################

database  bdb
suffix      "dc=tripplite, dc=com"
rootdn      "cn=Manager,dc=tripplite, dc=com"
rootpw      secret
directory   ./data
```

3. Restart the LDAP server.
4. Write the LDIF file and create the database entries in init.ldif with the *ldapadd* command, as shown in the following example:

```
ldapadd -f init.ldif -x -D “cn=Manager,dc=trip
plite,dc=com” -w secret
```

User Management

This page is used to set up and manage user profiles. It defines the access rights of each user. Up to 64 user profiles can be established

The settings on this page are described below:

Adding a User Profile

To add a user profile, fill in the information in the right panel of the screen and click **Add**. The new user's name appears in the User List.

Deleting a User Profile

To delete a user profile, select the desired profile from the User List and click **Remove**. The user's name is removed from the panel.

Editing a User Profile

To edit a user profile, you must first select the desired profile from the user list. The user information will be displayed in the right panel of the screen. Edit this information and click **Update**. If you do not click the **Update** button, your changes will be lost.

Note: For security purposes, the Password *and* Confirm *fields are not displayed. If you do not want to change the user's password, simply leave the two fields as is. If you do want to change the user's password, key in the new password in the* Password *and the* Confirm *fields.*

- The *Reset* button clears all the user profile information in the right panel of the screen.
- When you have made all your changes, click **Apply**. In order for your changes to be saved, the *Apply* button must be clicked. When editing a user profile, both the *Update* button and the *Apply* button must be clicked.

An explanation of the user profile items is given in the table below:

Item	Description
Username	A minimum of 6 and a maximum of 16 characters are allowed.
Password	A minimum of 6 and a maximum of 16 characters are allowed.
Confirm Password	To verify you have typed in the password correctly, you are asked to enter it again. If the two entries do not match, you will not be allowed to save the changes.
Description	This is an optional field that is used to record any additional information about the user profile.
Permissions	Click on a permission to add or remove access to a particular feature. You can choose to assign *Admin* permissions, *User* permissions or *Select* your own list of permissions. • Clicking on *Admin* will give the user access to all of the B051-000's features. The only permission box that will not be checked is the *View Only* permission. This is because *Admin* users will have full access to all computers/servers connected to the B051-000. • Clicking on *User* will give the user access to the *Win Client, Java Applet* and *Virtual Media*. They will have full access to all computers/servers connected to the B051-000. *Users* will not be able to *Configure* the B051-000 or access the *Log Server*. • Clicking on S*elect* allows you to choose whatever permissions you want the user to have. When the *Admin* or *User* profiles are checked, clicking on any of the permission will automatically check the *Select* profile as well. **Win Client:** Checking *Win client* allows a user to access the B051-000 via the Windows Client software. **View Only:** Checking *View Only* allows a user to view the video of the computers/servers connected to the B051-000, but they are not allowed to perform any operations on the computers. **Virtual Media:** Checking *Virtual Media* allows a user to utilize the B051-000's Virtual Media feature. **Java Applet:** Checking *Java Applet* allows a user to access the B051-000 via the Java Applet software. **Configure:** Checking *Configure* gives a user Administrator privileges, and allows the user to set up and modify the B051-000's operating environment. **Log:** Checking *Log* allows a user to view the contents of the log file.

Customization

This page allows the Administrator to upgrade the firmware and to set *Timeout*, *Login failure*, and *Working mode* parameters.

An explanation of all Customization parameters except Firmware Upgrade is given in the table below. Firmware Upgrade is discussed in the section following this table.

Parameter	Explanation
Timeout	If the B051-000 doesn't receive any input from a computer that is accessing it with the Windows Client or Java Applet for the amount of time specified here, it ends the connection. The default is 3 minutes.
Login Failure	**Allowed:** Sets the number of consecutive failed login attempts that are permitted from a remote computer. The default is 5. **Timeout** - Sets the amount of time a remote computer must wait before attempting to login again after it has exceeded the number of allowed failures. The default is 3 minutes.
Working Mode	**Enable ICMP:** If *ICMP* is checked, the B051-000 can be pinged, and an IP address can be assigned with the ARP command. If it is not checked, the device cannot be pinged or assigned an IP address with the ARP command. *ICMP* is checked by default. **Enable Device List:** If this item is checked, the device will show up in the list of local B051-000 units on the AP Windows Client Connection screen. If it is not checked, it will not show up. It is checked by default. **Force All to Grayscale:** If this item is checked, the remote display for all users is changed to grayscale. This can speed up I/O transfer in low bandwidth situations. By default, this item is not checked. **Enable Browser:** If this item is checked, users are allowed access to the B051-000 from a browser. If this function is not enabled, users will not be able to log into the unit via their browser. It is checked by default. **Enable Multiuser:** If this item is checked, multiple users can log into the B051-000 at the same time. It is checked by default.
Mouse Sync Mode	**Automatic***:* If this item is checked, the B051-000 will automatically sync the remote and local mouse pointers. It is checked by default. *Note: This feature only supports USB mice on Windows and Mac (G4 or higher) systems. For all other configurations, we recommend that you select* Manual*.* **Manual:** If this item is checked, all mouse synching must be done manually with the Windows Client and Java Applet synching procedures. By default, this item is not checked. *Note: Sun systems must use the Manual setting. If you use the Manual setting it may also be necessary to make additional mouse movement settings.*
USB IO Settings	**OS:** When connecting to a computer or KVM switch with the USB connector for keyboard and mouse I/O, drop down the list to select the platform it uses. Choices are PC, Mac1, Mac2, and Sun. PC is the default OS. *Note: In general, Mac 1 works best with older Mac OS versions, whereas Mac 2 works best with newer ones. This may vary, however. If you encounter problems with one setting, try selecting the other one.* **Language**: When connecting to a computer or KVM switch with the USB connector for keyboard and mouse I/O, drop down the list to select the keyboard language it uses. English is the default language.
Reset	Some configuration changes only take effect after a B051-000 reset. These include changes on the Network page, a Log Server port change, enabling/disabling browser access and upgrading the firmware. For those changes, a check is automatically put in the *Reset on Exit* box. To have the changes take effect, log out and then log back in again. A wait of approximately 30 to 60 seconds is necessary before logging in following the reset. *Note: If the B051-000's performance degrades, reset it by putting a check in the* Reset on Exit *box, and then log out / log in.*

AP Operation

Upgrading the Firmware

New versions of the firmware files can be downloaded from our website as they become available. After downloading the new firmware file, do the following:

1. On the *Customization* page of the Admin Utility, click the *Browse* button.
2. In the *File Open* dialog box that appears, navigate to the directory that the downloaded firmware upgrade file is in. Select the file and click **Open**.

When you return to the Customization page, the file appears in the *Mainboard F/W* field.

3. Click **OK** to begin the upgrade.

The AP Java Client

The Java Client is provided to make the B051-000 accessible to all platforms. Systems that have JRE 6 Update 3 or higher installed can connect. If you don't already have Java, it is available for free download from Sun's Java web site (http://java.sun.com).

Starting Up

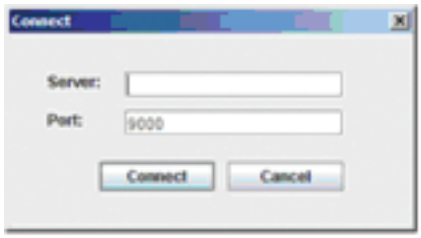
To connect to the B051-000 with the stand-alone Java Client program, copy the *iClientJ.jar* file from the B051-000 CD to a convenient location on your hard disk and then double-click its icon to bring up the Java Client connection screen.

Note: If this is the first time that you are running the program a dialog box appears requesting you to input your serial number.

The serial number can be found on the B051-000's CD case. This is not the same as the serial number that is on the bottom of the unit. You must use the serial number from the CD that came with the B051-000. Key in the serial number (5 characters per box) and click **OK** to bring up the B051-000 connection screen.

This dialog box will not appear after you have entered the serial number for the first time. You will go directly to the Java Client connection screen when starting up in the future.

The Java Client Connection Screen

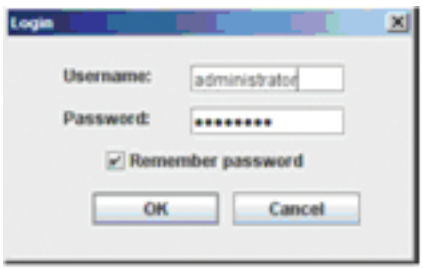


To connect to the B051-000:

1. Key in its IP address in the Server field.
2. Key in the correct port number.
3. Click **Connect**.

Logging In

Once the B051-000 connects to the unit you specified, a login window appears:



Provide a valid username and password and click **OK**.

Note: For Administrators accessing the B051-000 for the first time, the default username is administrator*; the default password is* password*. For security purposes, it is strongly recommended that you change these to something unique.*

After you have successfully logged in, a window opens on your desktop containing the remote server's display. This is the same window that appears when you run the browser-based Java Applet. Refer to Chapter 6, *The Java Applet*, for operational details.

Appendix

Specifications

Function	Specification
Console Connector	HD15 Male
Server/KVM Port	HD18 Female
Modem Connector	DB9 Male
LAN Port	RJ45 Female
Power Jack	DC Jack for Power Supply
Virtual Media Port	USB Mini-B Female
Reset Switch	Semi-Recessed Button on front-panel
Power LED	Orange
Link LED	Green
10/100Mbps LED	Orange (10Mbps), Green (100Mbps)

Function	Specification
Keyboard/Mouse Emulation	PS/2 and USB
Video Resolution	Up to 1600x1200 @ 60Hz; DDC2B
Power Consumption	5.3V, 6.3W
Operating Temperature	0° to 50° C
Storage Temperature	-20° to 60° C
Humidity	0-80% RH Non-Condensing
Housing	Metal
Weight	1.08lbs
Dimensions (LxWxH)	7.9in x 3.21in x 1in

PPP Dial-In Modem Operation

Basic Setup

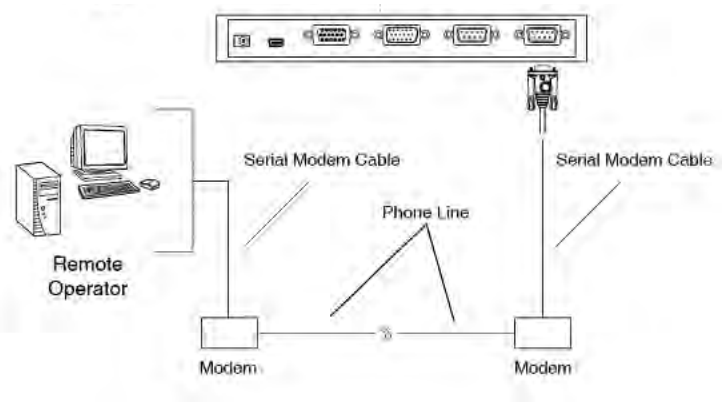
In the event the B051-000 is not accessible via the ordinary network connection, it can be accessed via PPP Dial-In Modem. Follow the instructions below to set-up and access the B051-000 via PPP Dial-In Modem.

1. Set-up your hardware configuration to match the diagram below. You will need to use a DB9 Serial Modem Cable to connect the DB9 port on the unit to your modem.
2. From your computer, use your modem terminal program to dial into the B051-000.

Note: If you don't know the B051-000 modem's serial parameters, get them from your System Administrator. An example of setting up a modem terminal program under Windows XP is provided in the following section.

3. Once the connection has been established, open your browser and specify the address *192.168.192.1.* From here, operation of the B051-000 is the same as if you had accessed it from the ordinary network.

Note: When accessing the B051-000 via PPP Dial-In Modem, video is automatically forced to grayscale and the Video Quality *setting is set at the lowest level.*



Connection Setup Example (Windows XP)

To set up a dial-in connection to the B051-000 under Windows XP, do the following:

1. From the Start menu, select **Control Panel Network Connections Create a New Connection.**
2. When the *Welcome to the New Connection Wizard* dialog box appears, click **Next** to move on.
3. In the *Network Connection Type* dialog box, select *Connect to the network at my workplace* and click **Next**.
4. In the *Network Connection* dialog box, select *Dial-up connection* and click **Next**.
5. In the *Connection Name* dialog box, key in a name for the connection and click **Next**.
6. In the *Connection Availability* dialog box, you can select either *Anyone's use or My use only,* depending on your preferences, then click **Next**.

Note: If you are the only user on this computer, this dialog box won't appear.

7. In the *Phone Number to dial* dialog box, key in the phone number of the modem connected to the B051-000 (be sure to include country and area codes, if necessary), then click **Next**.
8. In the *Completing the New Connection Wizard* dialog box, check *Add a shortcut to this connection on my desktop* and click **Finish**.

This completes the connection setup. Double click the desktop shortcut icon to make a dial-in connection to the B051-000.

Appendix

Troubleshooting

General Operation

Problem	Resolution
Erratic Operation.	• If the B051-000 is connected to a KVM switch, make sure to power on the switch before powering on the B051-000. • Press and hold the Reset button for longer than three seconds.
The Windows Client link doesn't appear in the *Remote Console Display* when I log in with Firefox.	The Windows Client link requires ActiveX. Since Firefox doesn't support ActiveX only the Java Applet is available.

The Java Applet

Problem	Resolution
Java Applet won't connect to the B051-000.	1. Java 6, Update 3 or higher must be installed on your computer. 2. Make sure to include the correct login string when you specify the B051-000's IP address. If a *Default web page name* is entered into the *Security Settings* screen (See page 17), you will need to type it in at the end of the B051-000 URL. 3. Close out of your browser and try again.
National language characters don't appear.	Use the B051-000's *On-Screen Keyboard* and make sure that the local and remote computers are set to the same language. (See *On-Screen Keyboard*, page 40.)
There is no Virtual Media icon on my Control Panel.	The virtual media function only supported by the Windows Client program.
When I log in, the browser generates a *CA Root certificate is not trusted or a Certificate Error* message.	The certificate can be trusted; click on the link that says 'Continue to this website (Not recommended).' (See page 12 for details.)

The Windows Client

Problem	Resolution
Windows Client won't connect to the B051-000.	DirectX 7.0 or higher must be installed on your computer.
When I log in, the browser generates a *CA Root certificate is not trusted or a Certificate Error* message.	The certificate can be trusted; click on the link that says 'Continue to this website (Not recommended).' (See page 12 for details.)
Part of remote window is off my monitor.	Use the *AutoSync* feature to sync the local and remote monitors.
Virtual Media doesn't work.	Make sure that the Virtual Media cable is properly connected. (See page 33.)

Mac Systems

Problem	Resolution
The local and remote mouse pointers do not sync.	There are two USB I/O settings for Mac computers. Mac 1 and Mac 2 (see *Customization*, page 27). In general, Mac 1 works with older operating system versions, and Mac 2 works with the newer ones. In some cases, however, the reverse is true. If you experience pointer sync problems, try selecting the other mode.

Sun Systems

Problem	Resolution
Video display problems with HD15 interface systems (e.g. Sun Blade 1000 servers).	The display resolution should be set to 1024 x 768: Under Text Mode: 1. Go to OK mode and issue the following commands: setenv output-device screen:r1024x768x60 reset-all Under XWindow: 1. Open a console and issue the following command: m64config -res 1024x768x60 2. Log out. 3. Log in.
Video display problems with 13W3 interface systems (e.g. Sun Ultra servers).	The display resolution should be set to 1024 x 768: Under Text Mode: 1. Go to OK mode and issue the following commands: setenv output-device screen:r1024x768x60 reset-all Under XWindow: 1. Open a console and issue the following command: m64config -res 1024x768x60 2. Log out. 3. Log in.
The local and remote mouse pointers do not sync.	The default configuration is for the local and remote mouse pointers to automatically sync when you connect; however, this is only supported by USB mice on Windows and Mac (G4 or higher) systems. You must select Manual as the Mouse Sync Mode choice, and sync the pointers manually.

Appendix

Troubleshooting *(continued)*

The Log Server

Problem	Resolution
The Log Server program does not run.	The Log Server requires the Microsoft Jet OLEDB 4.0 driver in order to access the database. This driver is automatically installed with Windows ME, 2000 and XP. For Windows 98 or NT, you will have to go to the Microsoft download site: http://www.microsoft.com/data/download.htm to retrieve the driver file MDAC 2.7 RTM Refresh (2.70.9001.0). Since this driver is used in Windows Office Suite, an alternate method of obtaining it is to install Windows Office Suite. Once the driver file or Suite has been installed, the Log Server will run.

Mouse Synchronization Tips

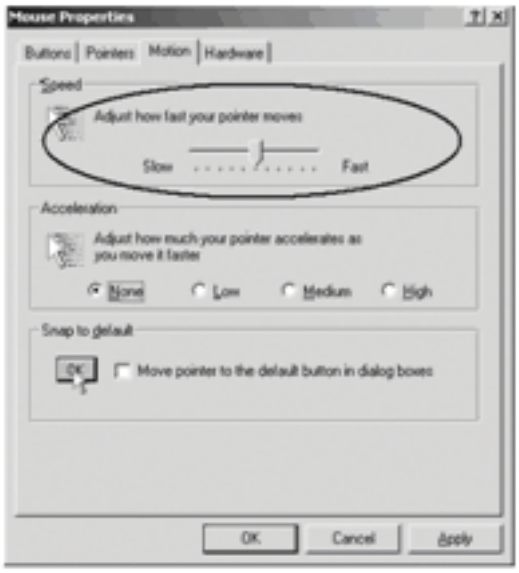
Before trying any mouse synchronization procedures, it is always a good idea to ensure that you go to your *Mouse Properties Settings* and set them according to the following:

Windows

Note: In order for the local and remote mice to synchronize, you must use the generic mouse driver supplied with the MS operating system. If you have a third party driver installed - such as one supplied by the mouse manufacturer - you must remove it.

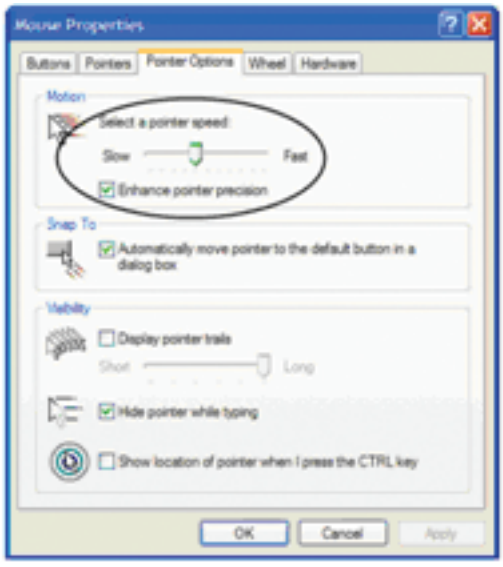
Windows 2000:

1. Open the Mouse Properties dialog box (**Control Panel → Mouse → Mouse Properties**)
2. Click the **Motion** tab.
3. Set the mouse speed to the middle position (6 units in from the left).
4. Set the mouse acceleration to *None*.



Windows XP / Windows Server 2003:

1. Open the Mouse Properties dialog box (**Control Panel → Mouse**)
2. Click the **Pointer Options** tab.
3. Set the mouse speed to the middle position (6 units in from the left).
4. Disable *Enhance Pointer Precision*.



Windows ME:

- Set the mouse speed to the middle position and disable mouse acceleration. (Click the *Advanced* button to get the dialog box for this).

Windows NT / Windows 98 / Windows 95:

- Set the mouse speed to the slowest position.

Appendix

Sun / Linux

Open a terminal session and issue the following command:

Sun: `xset m 1`

Linux: `xset m 0`

Mouse Sync Mode

In the *Customization Settings* screen there are two mouse sync modes; *Automatic* and *Manual*.

- **Automatic** is selected as the default, and will automatically sync the remote and local mouse pointers; however, this feature only supports USB mice on Windows and Mac (G4 or higher) systems. For all other configurations, we recommend that you select *Manual*.
- When **Manual** is checked, all mouse syncing must be done manually with the syncing procedures discussed in the following sections. Sun systems must use the Manual setting.

USB IO Settings

The *Customization Settings* screen contains a section called *USB IO Settings*, which can have an affect on mouse functionality. When connecting to a computer or KVM switch with the USB connector for keyboard and mouse, it is necessary to access the *OS* drop-down list in this section to select the OS platform being used. Choices are PC, Mac1, Mac2, and Sun. PC is the default OS.

Note: In general, Mac 1 works best with older Mac OS versions, whereas Mac 2 works best with newer ones. This may vary, however. If you encounter problems with one setting, try selecting the other one.

Adjust Mouse Hotkey

The Windows Client Control Panel contains a Hotkey (**Alt + M** by default) that syncs the local mouse pointer with the remote mouse pointer. Simply press the (**Alt + M**) Hotkey, and the local and remote mouse pointers should sync within a few seconds.

Auto-Sync Button

In the *Video Settings Menu* there is an *Auto-Sync* button that also server to sync the local and remote mouse pointers. In most cases, performing an *Auto-Sync* will align the two mouse pointers.

Video Quality Slider Bar

The *Video Settings Menu* also contains a slider bar that adjusts the quality of the video being displayed on the monitor. The higher the quality of the video, the more data is being passed through the network. Higher volumes of data will cause a delay in the time that it takes for your keyboard and mouse input to appear on the monitor. To decrease the quality of the video and improve response time, adjust the *Video Quality* slider bar to a lower setting.

Detect Tolerance Slider Bar

Also in the *Video Settings Menu*, the *Detect Tolerance* slider bar can be adjusted to limit the amount of information being sent through the network. If you are having problems with keyboard and mouse response time, setting the *Detect Tolerance* slider bar to high can help.

Grayscale

Another icon contained in the Windows Client Control Panel is the *Grayscale* icon. Clicking this icon will force the video on the monitor to be displayed in grayscale, which can reduce the amount of data traveling through the network, and improving keyboard and mouse response time.

Appendix

WARRANTY

1-YEAR LIMITED WARRANTY

Seller warrants this product, if used in accordance with all applicable instructions, to be free from original defects in material and workmanship for a period of 1 year from the date of initial purchase. If the product should prove defective in material or workmanship within that period, Seller will repair or replace the product, in its sole discretion. Service under this Warranty can only be obtained by your delivering or shipping the product (with all shipping or delivery charges prepaid) to: Tripp Lite; 1111 W. 35th Street; Chicago IL 60609; USA. Seller will pay return shipping charges. Visit www.tripplite.com/support before sending any equipment back for repair.

THIS WARRANTY DOES NOT APPLY TO NORMAL WEAR OR TO DAMAGE RESULTING FROM ACCIDENT, MISUSE, ABUSE OR NEGLECT. SELLER MAKES NO EXPRESS WARRANTIES OTHER THAN THE WARRANTY EXPRESSLY SET FORTH HEREIN. EXCEPT TO THE EXTENT PROHIBITED BY APPLICABLE LAW, ALL IMPLIED WARRANTIES, INCLUDING ALL WARRANTIES OF MERCHANTABILITY OR FITNESS, ARE LIMITED IN DURATION TO THE WARRANTY PERIOD SET FORTH ABOVE; AND THIS WARRANTY EXPRESSLY EXCLUDES ALL INCIDENTAL AND CONSEQUENTIAL DAMAGES. (Some states do not allow limitations on how long an implied warranty lasts, and some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitations or exclusions may not apply to you. This Warranty gives you specific legal rights, and you may have other rights which vary from jurisdiction to jurisdiction).

Tripp Lite; 1111 W. 35th Street; Chicago IL 60609; USA

WARNING: The individual user should take care to determine prior to use whether this device is suitable, adequate or safe for the use intended. Since individual applications are subject to great variation, the manufacturer makes no representation or warranty as to the suitability or fitness of these devices for any specific application.

WARRANTY REGISTRATION

Visit www.tripplite.com/warranty today to register the warranty for your new Tripp Lite product. You'll be automatically entered into a drawing for a chance to win a FREE Tripp Lite product!*

* No purchase necessary. Void where prohibited. Some restrictions apply. See website for details.

Warning!

Use of this equipment in life support applications where failure of this equipment can reasonably be expected to cause the failure of the life support equipment or to significantly affect its safety or effectiveness is not recommended. Do not use this equipment in the presence of a flammable anesthetic mixture with air, oxygen or nitrous oxide.

WEEE Compliance Information for Tripp Lite Customers and Recyclers (European Union)

Under the Waste Electrical and Electronic Equipment (WEEE) Directive and implementing regulations, when customers buy new electrical and electronic equipment from Tripp Lite they are entitled to:

- Send old equipment for recycling on a one-for-one, like-for-like basis (this varies depending on the country)
- Send the new equipment back for recycling when this ultimately becomes waste

FCC Part 68 Notice (United States Only)

If your Modem/Fax Protection causes harm to the telephone network, the telephone company may temporarily discontinue your service. If possible, they will notify you in advance. If advance notice isn't practical, you will be notified as soon as possible. You will be advised of your right to file a complaint with the FCC. Your telephone company may make changes in its facilities, equipment, operations or procedures that could affect the proper operation of your equipment. If it does, you will be given advance notice to give you an opportunity to maintain uninterrupted service. If you experience trouble with this equipment's Modem/Fax Protection, please visit www.tripplite.com/support for repair/warranty information. The telephone company may ask you to disconnect this equipment from the network until the problem has been corrected or you are sure the equipment is not malfunctioning. There are no repairs that can be made by the customer to the Modem/Fax Protection. This equipment may not be used on coin service provided by the telephone company. Connection to party lines is subject to state tariffs. (Contact your state public utility commission or corporation commission for information.)

Tripp Lite follows a policy of continuous improvement. Product specifications are subject to change without notice.

Tripp Lite World Headquarters
1111 W. 35th Street, Chicago, IL 60609 USA
www.tripplite.com/support

200909083 93-2850